Next Generation 911 Cost Estimate

A Report to Congress

October 2018

To the reader:

Pursuant to section 6508 of the Next Generation 9-1-1 Advancement Act of 2012 (the Act), we are pleased to submit this Next Generation 911 (NG911) Cost Estimate Report (Report). The Report analyzes and determines detailed costs for NG911 service requirements and specifications. As required by the Act, the Implementation Coordination Office (ICO), which is jointly administered by the National Highway Traffic Safety Administration (NHTSA) and the National Telecommunications and Information Administration (NTIA), consulted with the Federal Communications Commission and the Department of Homeland Security in preparing the Report. The NG911 Cost Estimate Report provides a feasibility life-cycle cost estimate of the scope that would enable migration from existing legacy 911 systems to NG911. The Report describes the implementation of this scope using three different implementation scenarios, with the bounds of the cost range reflecting the lowest and highest cost amounts from these scenarios.

It is important to note that while the Report explores geographic cost allocation of NG911 implementation, it does not detail the cost breakdown between localities, States, and federal agencies. In addition, the Report does not quantify various other elements that may substantively increase or decrease the range, including fees received by 911 agencies during the implementation period, any technological advancements that may provide efficiency in implementation, or changes in Public Safety Answer Points that may result during implementation.

The NG911 lifecycle cost estimate range, shared between localities, States and federal agencies, is between $13.5 and $16 billion (including equipment refresh costs and ongoing operational costs), and the cost estimate range for NG911 deployment is between $9.5 and 12.7 billion. The time-period for the implementation estimate is ten years, assuming no scheduling delays, no funding delays, and no deviations from the recommended implementation path. NHTSA and NTIA are committed to supporting 911 as a vital service to maintain the security and safety of the American people. If you have any questions about this report, please contact nhtsa.national911@dot.gov.

Sincerely yours,

Heidi R. King
Deputy Administrator
National Highway Traffic Safety
Administration

David J. Redl
Assistant Secretary of Commerce for
Communications and Information and
National Telecommunications and
Information Administration Administrator

EXECUTIVE SUMMARY

OVERVIEW OF THIS REPORT

As requested by Congress, this Report presents a feasibility estimate of the costs to implement Next Generation 911 (NG911) service nationwide. This Report is intended to assist Congress in considering whether to develop a long-term funding mechanism to support NG911 system implementation, the operation and maintenance of such systems, and the training of personnel who will be using these systems. This report strives to provide an understanding of the complexity of NG911 implementation, the extent of NG911 implementation to date, and the required steps necessary to achieve the desired end state of NG911 deployment. While the intended audience and scope is at the national level, portions of the study will benefit the public safety and 911 stakeholder community at all levels.

The Report was prepared by the 911 Implementation Coordination Office (which is jointly administered by the National Highway Traffic Safety Administration (NHTSA) and the National Telecommunications and Information Administration (NTIA)), in consultation with the Federal Communications Commission (FCC), and the Department of Homeland Security (DHS).

THE CRITICAL IMPORTANCE OF NEXT GENERATION 911 TO THE NATION

The first 911 call was made nearly 50 years ago, in February 1968, in Haleyville, Alabama. This universal emergency number was created to ensure that anyone in the United States could quickly and easily dial public safety for help. Today, the 911 system is a critical service providing access to public safety and first responders in any time of need. In 2016, over 250 million calls were delivered to 911 centers across the country.

Since that first 911 call, communication forms have become increasingly digital — texts, photos, videos, and Voice over Internet Protocol (VoIP) — and many "phone" systems rely on technologies that have become obsolete and unserviceable. But the 911 systems used by public safety professionals to assist the public continue to rely heavily on these older technologies. Public safety and industry leaders agree that upgrading to Next Generation 911 (NG911) systems across the country is needed to ensure that every request for emergency help can be received, located, and responded to in the way that best meets the needs of the public and first responders.

NG911 systems represent a leap forward for emergency response operations in the U.S. Because NG911 systems are Internet Protocol (IP)-based and broadband-enabled, they make it possible for 911 telecommunicators and first responders to receive not only voice calls but also data relevant to an emergency-- such as photos, streaming video, and even building plans. Being able to receive and process such data – which is simply not possible with legacy 911 systems – will provide first responders with more complete real-time information and thereby make them more effective in responding to emergencies. This will lead to faster response and more lives and property saved— and will make both the public and first responders themselves safer. NG911 systems can also integrate state-of-the-art network design to facilitate 911 calls being transferred and rerouted when individual 911 call centers are inundated with high call volumes or experience technical problems such as power outages in major disasters. These network capabilities – another significant improvement over legacy 911 -- will vastly increase the resilience and reliability of the 911 system.

NG911 will allow the nation's 911 systems to:

- meet the communication needs and expectations of the public
- deliver reliable, resilient, redundant emergency communication services to communities nationwide
- enable seamless integration with the Nationwide Public Safety Broadband Network (NPSBN)—which is being implemented under the auspices of the First Responder Network Authority (FirstNet)—creating a unified digital public safety communications ecosystem

The LCCE report presented is a comprehensive parametric estimate for the deployment of NG911 systems based on the NG911 cost study functional requirements, technical requirements, and specifications. The evaluation of the current NG911 environment summarized in the NG911 current status was a primary input for this analysis, ensuring that the cost model only estimates the additional cost of bringing states and territories to the NG911 end state. Therefore, costs of operating and maintaining the currently fielded 911 systems (legacy or NG911) are outside the scope of this study.

The geographical scope of this study includes the entire U.S. and its territories, divided into FEMA regions. The SMEs established a ten-year time period of analysis, selecting 2017 as the base year of this analysis.

The analysis consisted of three major implementation scenarios: 1) individual state implementation, 2) multistate implementation, and 3) service solution.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

CONGRESSIONAL DIRECTIVE TO COMPLETE A NEXT GENERATION 911 COST STUDY

The migration from existing legacy 911 systems to NG911 will be an enormous and costly endeavor. Experts agree it is essential and will lead to a safer and more effective 911 system for the public and first responders. To help determine the cost of this migration, Congress directed the 911 Implementation Coordination Office to prepare this Report. Congress also directed that this Report include:

- how costs would be broken out geographically and allocated among public safety answering points, broadband service providers, and third-party providers of NG911 services

- an assessment of the current state of NG911 service readiness among public safety answering points

- how differences in public safety answering points' access to broadband across the United States may affect costs

- a technical analysis and cost study of different delivery platforms, such as wireline, wireless, and satellite

- an assessment of the architectural characteristics, feasibility, and limitations of NG911 service delivery

- an analysis of the needs for NG911 services of persons with disabilities

- standards and protocols for NG911 services and for incorporating Voice over Internet Protocol and ''Real-Time Text'' standards

KEY ELEMENTS OF THIS REPORT

The *Next Generation 911 Cost Estimate – A Report to Congress* provides an assessment of the current 911 service environment and the future NG911 architecture, in addition to a detailed estimate concerning the costs to bring next-generation service to the Nation's 6,000-plus public safety answering points (PSAPs), also known as 911 call centers.

The methodology utilized to complete this Report included the development of a maturity model to assess the current status of NG911 implementation nationwide, the incorporation of actual deployment and cost data into the model, and the formulation of an NG911 architecture as the desired end state for deployment. This process resulted in a range of costs to achieve nationwide end state NG911 implementation, based on a group of assumptions, related to economic, administrative, technical, and operational factors.

The high-level ground rules and assumptions that were utilized in conducting this cost analysis included:

- Costs of operating and maintaining the current legacy 911 systems are not included within this analysis
- Achieving the desired NG911 end state is scheduled for all states and territories within ten years of initiation, starting from their current state of operation

- The costs associated with federally operated PSAPs (e.g., Department of Defense) are not included in this report
- For optimal organization at the nationwide level, each state should have a single authoritative entity for its NG911 network
- States will be responsible for implementing and maintaining their own infrastructure; therefore, consolidations and shared infrastructure, while important, are out of scope
- The current number of PSAPs is sufficient to serve the population of each respective region/municipality
- Cost data sources include publicly available data from NG911 estimates, vendor information, government contracts, and other publicly available cost information at a state or multistate level

This report considered three NG911 implementation scenarios:

- State Implementation—States and territories independently would implement an ESInet, which is the transport medium for NGCS, the suite of solutions that enable PSAPs to field and process voice, text, and data calls in an NG911 environment. Each state and territory would implement at least one statewide ESInet, and a minimum of two redundant NGCS centers.
- Multistate Implementation—Multiple states within ten geographical areas—which generally correspond to the Federal Emergency Management Agency (FEMA) regions— would coordinate their NG911 implementation efforts, largely by interconnecting their statewide ESInets and leveraging NGCS provided by shared, mega-sized centers.
- Service Solution—Each state and territory independently would utilize a contracted service provider that would provide all core services and NG911 system maintenance.

1.   BACKGROUND

The National 911 Program conducted a Next Generation 911 (NG911) Cost Study that "analyzed and determines detailed costs" for a nationwide implementation of NG911, as required by Congress in the Middle Class Tax Relief and Job Creation Act of 2012 (P.L. 112-96).

The Middle Class Tax Relief and Job Creation Act of 2012 directs the Implementation Coordination Office (today known as the National 911 Program)—in consultation with the National Highway Traffic Safety Administration (NHTSA), the Federal Communications Commission (FCC), and the Department of Homeland Security (DHS) to submit a report to Congress analyzing and determining detailed costs for specific NG911 service requirements and specifications.

By statute, "the purpose of the report is to serve as a resource for Congress as it considers creating a coordinated, long-term funding mechanism for the deployment and operation, accessibility, application development, equipment procurement, and training of personnel for Next Generation 911 services." The report also must include the following:

- How costs would be broken out geographically and allocated among public safety answering points, broadband service providers, and third-party providers of Next Generation 9-1-1 services
- An assessment of the current state of Next Generation 9-1-1 service readiness among public safety answering points
- How differences in public safety answering points' access to broadband across the United States might affect costs
- A technical analysis and cost study of different delivery platforms, such as wireline, wireless, and satellite
- An assessment of architectural characteristics, feasibility, and limitations for Next Generation 9-1-1 service delivery
- An analysis of the needs for Next Generation 9-1-1 services of persons with disabilities
- Standards and protocols for Next Generation 9-1-1 services and for incorporating Voice over Internet Protocol and "Real-Time Text" standards[1]

This report provides the results of the ten-year lifecycle cost estimation (LCCE) of the nationwide implementation of NG911. The results contained herein are provided as a cost estimate for the entire United States (U.S.), including territories, except federally operated public safety answering points (PSAPs). Federal agencies that operate PSAPs must complete their own planning and budgeting process according to the agency's policies. The agency must properly plan to ensure the capability to exchange vital information with other federal and non-federal PSAPs.

In the U.S., the provisioning of 911 service traditionally has been focused at the local level. Each local 911 authority would contract with its local provider for the level of 911 service that was available. Over the years, as the industry matured, more states and agencies developed 911 rules and definitions, as well as funding mechanisms, that have left the scope of 911 not clearly agreed upon. Many states define 911 as receiving a call from the public networks, but do not include the dispatch function in their definition, even though the function is performed by the PSAP. In some cases, if it is not included in the definition, it is not eligible for funding. Other states include some of the dispatching equipment, but not staffing. Other states will allow all PSAP costs and some even allow costs associated with the responders' communications equipment.

---

[1] *Middle Class Tax Relief and Job Creation Act of 2012,* Public Law 112-96, 112th Cong., 2012, sec. 6508(c).
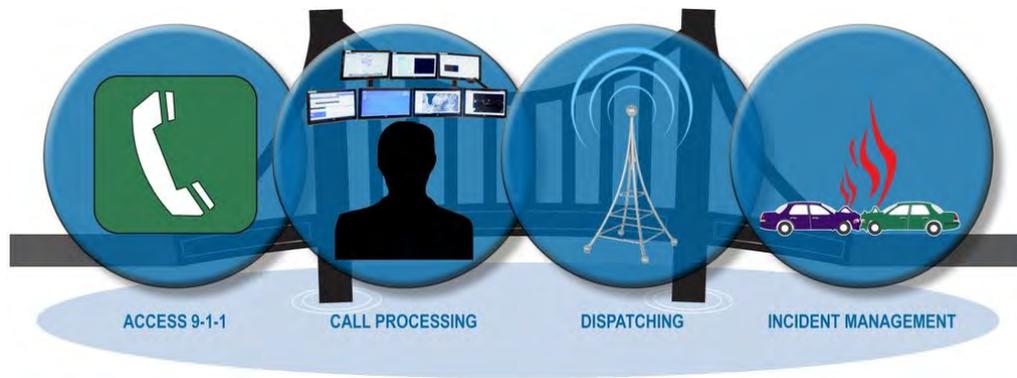
Figure 1: 911 Interconnected Systems

The public does not see these interconnected systems; they call 911 and expect to get help when and where they need it. For this cost study, the architecture, maturity model and cost models were developed on the complete system of systems, from the caller to the responder.

1.1.   Purpose

This report provides information to meet the intended purpose as stated in the public law: "to serve as a resource for Congress as it considers creating a coordinated, long-term funding mechanism for the deployment and operation, accessibility, application development, equipment procurement, and training of personnel for Next Generation 9-1-1 services."[2]

The data and information is focused on a nationwide scope and is consolidated. The result is a picture of the total cost, but an inability to separate the data out to a single entity or state; as such, the audience is national-level elected officials and their staff, as well as officials from federal departments and agencies.

This report strives to provide the reader with an understanding of the complexity of NG911 implementation and the extent of the interconnections. While the intended audience and scope is at the national level, portions will benefit the public safety and 911 community at all levels. The NG911 Maturity Model can be used to measure progress towards NG911 at all levels.

---

[2] *Middle Class Tax Relief and Job Creation Act of 2012,* Public Law 112-96, 112th Cong., 2012, sec. 6508(b).

1.2.   NG911 is Transformational Change

The implementation of NG911 nationwide represents a transformational change. Meanwhile, the history of 911 has been full of lesser transitions and incremental updates since its beginning. While transitions and updates traditionally have been accomplished at the local or regional level, NG911 transformational change requires all levels—up to and including the state and nationwide levels— as well as non-911 entities, to work collaboratively.

NG911 becomes a system of systems that requires detailed coordination for connection between the systems, and cooperative agreements between the entities to share data. Changes become more complicated; where before a provider only would notify its customers when a change occurred, in an NG911 environment, these systems connect to other systems beyond the primary customers, which increases operational complexities. Even a simple device software change can have a large impact on other systems.

To understand the adoption of NG911 as transformational change, it is helpful to utilize the Innovation Adoption Lifecycle, which describes the adoption or acceptance of a new product or innovation, such as NG911, according to the demographic and psychological characteristics of defined adopter groups. The process of adoption over time typically is illustrated as a classic normal distribution or bell curve. The model indicates that the first group of people to use a new product is called "innovators," followed by "early adopters."

Those areas that began the NG911 transition, sometimes in advance of standards being completed, are the innovators and early adopters. States like Indiana and Vermont fall into the innovator category, with states like Alabama, Iowa, and Tennessee being early adopters. Next come the early majority and late majority, and the last group to eventually adopt a product is called laggards. Figure 5 below depicts the groups and percentages involved in the Innovation Adoption Lifecycle.

Figure 2: Innovation Adoption Lifecycle

In addition to the challenges of the normal transition to new technologies, NG911 technologies are shared by, and interconnected to, other jurisdictions. This sharing of resources, and interconnection, on such a large scale is still new to public safety, a sector that has been siloed and jurisdictionally based for so long. The need to adopt new policies and procedures, and to interoperate with various new systems, will transform the 911 system of the future.

Table 1: NG911 Current Status

	Legacy	Foundational	Transitional	Intermediate	End State
Business Domain	73.6%	16.4%	2.9%	7.1%	
Data Domain	89.0%		8.2%	2.8%	
Applications and Systems Domain	79.2%	10.0%	1.0%	9.8%	
Infrastructure Domain	88.2%	10.2%		1.6%	
Security Domain	86.9%	7.1%	6.0%		
Operations/ Performance Domain	98.0%	2.0%			

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

The nationwide NG911 Maturity Model current status (NG911 current status), identified in Table 3 above, displays the percentage of the population serviced by 911 authorities that have implemented elements of the NG911 Maturity Model. Looking at the percentage beyond the legacy stage shows the percentage of adoption for that domain.

This table shows that the percentage of population beyond the legacy level in the Business Domain is well into the early majority, as defined by the Innovation Adoption Lifecycle, with 26.4 percent of the nation beginning to adopt NG911. The next largest domain is Applications and Systems, which is also into the early majority, with 20.8 percent of the nation beginning to adopt NG911. Additional implementations in the Infrastructure, Data, and Security domains are in the early adopters, but have begun. The laggard seems to be the Operations/Performance Domain, which is understandable as many of the systems are still in the implementation or early service life phases.

1.3.   Data Sources

Available data from the National Profile Database, the FCC, and other open sources was used as a resource to compile this report. As explained in more detail in Section 2.2 – Framework and NG911 Maturity Model, the Team gathered National Profile Database and FCC data using the high-level definition of NG911 readiness and the current understanding of the three stages of early adoption. Therefore, the data for the functional components was compiled and interpreted using firsthand knowledge of NG911 transitional activities by industry subject-matter experts (SMEs).

The percentages listed in the NG911 current status table (Table 3 above) represent the estimated portion of the national population that is covered by the systems that meet the definitions of the NG911 Maturity Model for the functional component and stage listed.

The Team collected cost data from available open sources, such as previous NG911 cost studies, public contracts and reports—such as 911 authority progress reports—and annual budgets. In addition, a limited number of current vendors contributed to the report by providing their manufacturers' recommended prices for their services on a confidential basis. This mix of cost data then was broken into pricing by the Team for the specific hardware, software and service items identified within each functional element of the NG911 Maturity Model.

In addition, the Team used statistical data for state-level populations, population density, and number of counties in a state gathered from the 2010 U.S. Census, as well as factors and characteristics related to the Federal Emergency Management Agency (FEMA) geographical

regions, to assist in creating the cost projection. This is explained in further detail in Section 4.1 – Data Sources.

1.4.   Scope

The purpose of the analysis conducted by the Team was to generate a range of costs for the planning, acquisition, implementation, and sustainment of NG911 systems for the U.S. and its territories. This study uses data at the state level when available, but a lack of individual state analysis restricts accurate projections of individual state funding levels. Therefore, it is not intended to develop locality system requirements or budget needs, nor to serve as a funding decision analysis for any individual state. In addition, the Team assumed for this report that states will maintain their current levels of PSAPs and dispatching systems. Therefore, any consolidations and/or shared infrastructure, while important, are out of scope for this study.

The LCCE report presented is a comprehensive parametric estimate for the deployment of NG911 systems based on the NG911 cost study functional requirements, technical requirements, and specifications. The evaluation of the current NG911 environment summarized in the NG911 current status was a primary input for this analysis, ensuring that the cost model only estimates the additional cost of bringing states and territories to the NG911 end state. Therefore, costs of operating and maintaining the currently fielded 911 systems (legacy or NG911) are outside the scope of this study.

The geographical scope of this study includes the entire U.S. and its territories, divided into FEMA regions. The SMEs established a ten-year time period of analysis, selecting 2017 as the base year of this analysis.

The analysis consisted of three major implementation scenarios: 1) individual state implementation, 2) multistate implementation, and 3) service solution.

Table 2: NG911 Implementation Scenarios

Scenarios	Description
State Implementation	Fully independent states and territories with a minimum of two Next Generation Core Services (NGCS) centers
Multistate Implementation	Multiple states within ten geographical areas coordinate and leverage from shared, mega-sized NGCS centers
Service Solution	Fully independent states utilize an NG911 service provider for all core services and PSAP system maintenance

The first alternative includes a single set of NGCS centers for each state. This is represented as a minimum of two physically and geographically redundant NGCS centers in the investment and operational cost requirements for each state within a region. For the second alternative, the assumption changes to a set of ten geographic areas in which multiple states share two NGCS centers among them. The third alternative shifts to a service solution acquisition method. These alternatives are described in more detail within Section 4 – Cost Analysis Framework.

This page is intentionally left blank.

2.   NG911 ARCHITECTURE

2.1.   Description

NG911 is an enterprise solution that will result in a nationwide system of systems that must share a common approach and be interoperable. The NG911 architecture for the cost study, shown in Figure 6 below, depicts a high-level view of a complete NG911 continuum, including legacy, transitional, and end state components. Transitional elements such as the legacy gateways and Internet Protocol (IP) selective router (IPSR) will be decommissioned when the end state is reached, or as legacy originating and terminating systems are decommissioned. (Appendix A, Section A.2 – Architecture contains an enlarged version of the diagram.)
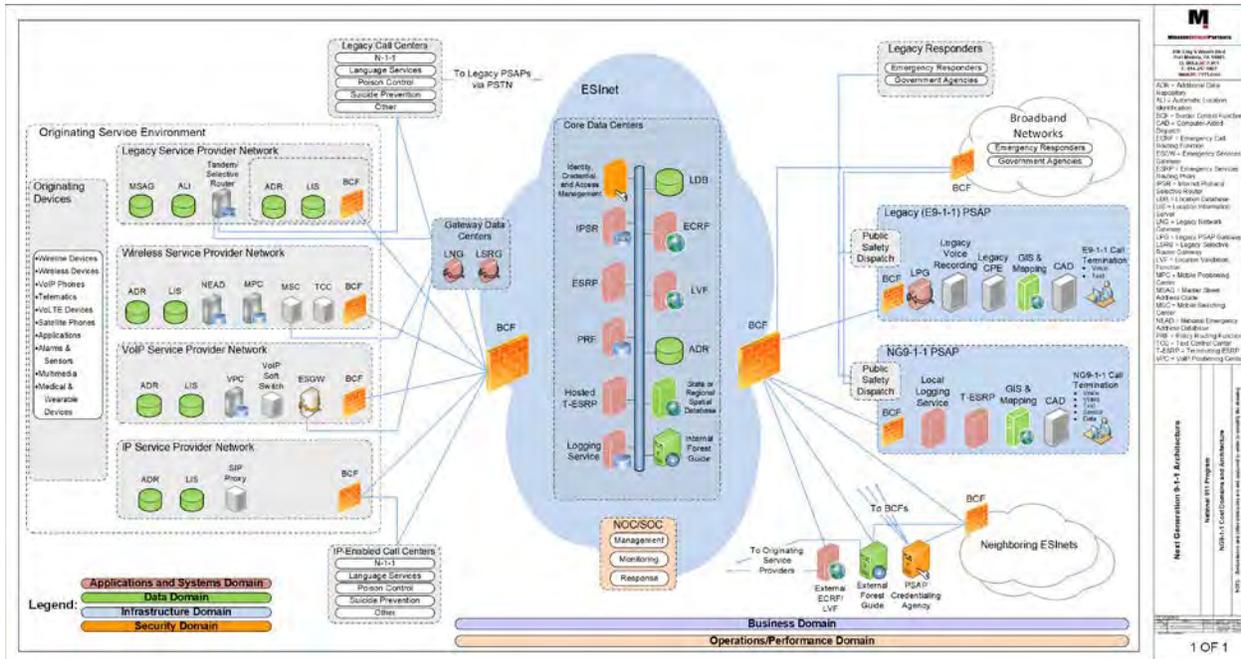
Figure 3: NG911 Architecture

The NG911 architecture used to produce the cost analysis is a combination of the cost study architecture and the NG911 Maturity Model.

All components of the NG911 cost study architecture are included in the NG911 Maturity Model; however, the model adds the stages of deployment. The NG911 Maturity Model was the basis of the cost analysis to determine the cost elements and timing of deployments throughout the ten-year lifecycle. The NG911 Cost Study architecture is described below.

2.1.1. *Originating Service Environment*

The originating service environment (OSE) consists of the devices and systems necessary to establish a call or request for service. For the purposes of this document, the term "call" refers to any request regardless of the form it takes or the technology employed to deliver information to a PSAP. This includes wireline, wireless, and Voice over IP (VoIP) voice calls; teletypewriter/telecommunications device for the deaf (TTY/TDD) calls; alarms; telematics; text messaging; and any other technology that may be used to report an emergency.

Originating devices may take many forms: telephones, private branch exchanges (PBXs), unified communications (UC) systems, smartphones, tablets, personal computers (PCs), alarm systems, sensors, wearables enabled with sensors, Internet of Things (IoT) devices, vehicles, healthcare devices, and machines.

To deliver a 911 call from a legacy provider, the legacy service provider network has an IP connection to allow access from the Emergency Services IP network (ESInet) to a provider-based Additional Data Repository (ADR) and Location Information Server (LIS). The Master Street Address Guide (MSAG) and automatic location identification (ALI) services may be accessed via Time Division Multiplexing (TDM) connections or an IP connection. The legacy service provider network will send calls to the ESInet via TDM connections to a Legacy Network Gateway (LNG), which will perform a variety of functions to provide compatibility with the NGCS within the ESInet. Additionally, the legacy service provider network connects to the ESInet's Legacy Selective Router Gateway (LSRG) to enable interoperability between legacy PSAPs that are not served by an ESInet and PSAPs—both legacy and NG911—that are served by an ESInet.

To deliver a call from a wireless provider, the wireless service provider network has an IP connection to allow access to the ESInet for a provider-based ADR, LIS, Mobile Positioning Center (MPC), Text Control Center (TCC), or Mobile Switching Center (MSC). In most cases, initially, MSCs will connect to the ESInet via TDM connections through an LNG. Over time, MSCs will migrate to an IP connection to the ESInet.

The VoIP Service Provider (VSP) network has an IP connection to allow access from the ESInet to a provider-based VoIP Positioning Center (VPC), ADR and LIS. VoIP calls will be delivered to the ESInet via TDM connections from VSP Emergency Services Gateway to an LNG, or over an IP connection.

The IP service provider network will connect to the ESInet via an IP connection for interfacing its ADR, LIS, and future systems.

Call centers, both TDM-based and IP-based, are shown outside the OSE, with connections to both the OSE and the ESInet/PSAP environment. These centers seldom will truly originate a call, but frequently will be a party to a 911 call.

2.1.2.   NG911 Core and ESInet

During the Foundational and Transitional stages, TDM traffic will be delivered from the legacy providers to gateway data centers for conversion to Session Initiation Protocol (SIP) by LNGs. When the Intermediate stage is reached, the incoming gateways will be decommissioned. The ESInet provides the underlying transport for the services and systems that will handle the emergency calls. Border Control Functions (BCFs) provide security for the ESInet and protection for incoming and outgoing IP traffic. The network operations center (NOC) and security operations center (SOC), which may be combined or separate facilities, monitor the health and security of the network, provide problem and change management functions, report as required on all aspects of the status and health of the network and its systems and services, and coordinate response to system or network issues.

The services within the core data centers collectively are referred to as NGCS. These are the services required to process a call from its entry into the ESInet to its delivery to the PSAP workstation. The IPSR is a transitional element providing SIP-based routing functions using legacy MSAG and ALI records. This element is decommissioned at the end of the Transitional stage. Some PSAPs may migrate directly to the Intermediate stage, bypassing the use of an IPSR.

The Emergency Services Routing Proxy (ESRP) also provides call-routing functionality, but relies on queries to geospatial data in the Emergency Call Routing Function (ECRF). There may be multiple ESRPs involved in routing a call to the proper PSAP. Call-handling systems considered to be compliant with the National Emergency Number Association (NENA) i3 standards often are referred to as Terminating ESRPs (T-ESRPs), because they use the same methodology as an ESRP to route the call to a specific telecommunicator for call handling. There also may be a hosted instance of a call-handling system, where the back-office systems are in the core data centers and only the workstations are at the PSAP.

The ECRF queries its geographic information system (GIS) data using the location information provided in the SIP header information passed to it from the ESRP. In some cases, the ESRP may query another database to request newer location information. The ECRF then returns routing information that enables the ESRP to consult the Policy Routing Function (PRF) and properly route the call. The Location Validation Function (LVF) is a mirror image of the data that resides in the ECRF, and is queried by the LIS to validate civic location information prior to a call being placed.

The PRF is a database of special routing rules that typically reside in the ESRP, and which may override the routing instructions returned from the ECRF. Special rules for time of day, special events, natural disasters, and/or PSAP evacuations are configured and stored in the PRF. In the appropriate circumstances, a rule may be invoked to distribute calls from one PSAP queue to another PSAP queue, which may increase the ability to handle the calls.

The logging service maintains transaction records from every system or service that handles a given call, along with the media streams associated with the call. Locating the logging service within the NGCS data center allows for pre-answer recording of the media streams. This does not preclude any PSAP from maintaining a local logging service. Such a device may be utilized to log local event data in case the PSAP is severed from the ESInet and is working in a local survivability mode, where it is only receiving calls on administrative lines separate from the ESInet connection.

The Location Database (LDB) is a hybrid database that combines the functionality and interfaces of legacy ALI databases with the NG911 functionality and interfaces of the LIS and ADR. As a transitional element, it enables an i3 call flow in an environment where carriers continue to submit legacy Service Order Input (SOI) and do not yet provide their own LIS and ADR services.

The ADR and Identity Searchable (IS)-ADR contain additional information about a variety of subjects related to a given call, caller, or the call location. This may include, but is not limited to, subscriber information, medical information, building floor plans, and emergency contact information.

A local copy of state or regional GIS data also may be maintained within the NGCS, along with local instances of security, credential, and access management data. The state or regional GIS data will use a spatial interface to provide data updates to the elements using GIS data, such as the LVF, ECRF, call-handling system, and computer-aided dispatch (CAD) mapping application.

2.1.3. PSAPs

The legacy PSAP has customer premises equipment (CPE) that is not capable of handling SIP or i3 calls. A legacy PSAP gateway (LPG) connects the PSAP to the ESInet, allowing SIP calls to be routed to the PSAP. The LPG is protected by a BCF instance. The legacy PSAP may maintain TDM connections to its service providers until the CPE is upgraded to an i3-capable call-handling system. The legacy PSAP will have connectivity to legacy responders for dispatching resources to a call incident.

The NG911 PSAP is an all-IP, i3-capable PSAP. This PSAP is depicted with the call-handling system (T-ESRP) residing locally at the PSAP. The NG911 PSAP may have connectivity to both legacy-enabled responders and IP-enabled responders, such as those served by the Nationwide

Public Safety Broadband Network (NPSBN) being implemented by the First Responder Network Authority (FirstNet).

2.1.4. Other Supporting Systems

The National Emergency Address Database (NEAD) is a developing solution that will enable mobile devices to provide a dispatchable location; it is designed specifically to resolve issues and mitigate challenges associated with locating wireless callers indoors and in multitenant buildings. The NEAD will house detailed location information for Wi-Fi access points and Bluetooth beacons, including street address, floor, suite, apartment, and other location information. The NEAD has an IP connection to the ESInet.

The Forest Guide is a repository of location and routing information that may be queried to determine suggested call routing for a call that cannot be routed by the local or regional routing data. The PSAP credentialing agency provides and authenticates security credentials for the various components of the NGCS and PSAPs.

2.2.   Framework and NG911 Maturity Model

The 911 stakeholder community reached a consensus that NG911 implementations must be standards-compliant. In instances where standards do not exist for elements within the NG911 Maturity Model, industry informational documents and best practices have been cited. The Team leveraged the current work being performed to maintain the NG911 Standards Identification and Review[3] document to begin developing the assessment of potential gaps in the NG911 architectural design.

To date, the transition to NG911 has been viewed in three main stages (see Figure 7 below), as identified by the National 911 Program's NG911 Transition Plan in 2009.[4]

---

[3] National 911 Program, *Next Generation 911 (NG911) Standards Identification and Review*, (March 2015), https://www.911.gov/pdf/NG911-Standards-Identification-and-Analysis-March2015.pdf.

[4] "Next Generation 9-1-1" U.S. Department of Transportation, http://www.its.dot.gov/factsheets/ng911.htm.

- The Legacy environment is where operations continue to use the current 911 networks of selective routers, ALI databases, and legacy protocol circuits to transmit voice and associated call data to the PSAP.
- The Transitional environment is where all other activities and systems between the two stages are lumped. This stage includes some minimal level of planning, and some moderate transition to IP networks has taken effect.
- The NG911 End State occurs when a state or region has deployed an IP network to each PSAP with complete deployment of standards-based NG911 systems, including IP call delivery from originating service providers (OSPs).
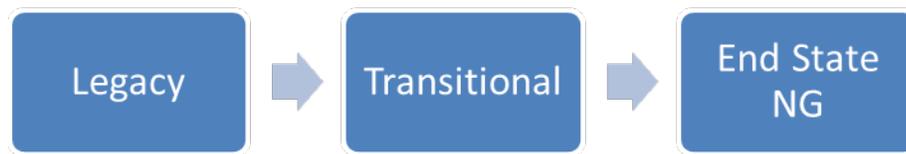
Figure 4: Historical View of NG911 Implementation

Increased understanding and progress in the deployment of NG911 has further fine-tuned the approaches to implementation, and thus generated a greater degree of granularity in understanding the current state of deployment for states/territories, regions, and PSAPs. With this expanded knowledge of implementation reality, it is appropriate to move from broad categories of implementation to more specific stages to fully understand the state of the nation. The result is a more mature view of the state of NG911 implementation, which is described in Section 2.3 below, NG911 Maturity Model.

A framework of readiness and deployment progress that can be used throughout the cost study and beyond was needed. It is commonly acknowledged that NG911 will be deployed in phases or stages, some components can be deployed independently of others, and some deployments are occurring today. The Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) Working Group 2 Report, *Optimal 9-1-1 Service Architecture*, states:

> *The Working Group does not believe there is a single best system design, but rather various options that may be selected representing an "optimal architecture" for each specific NG9-1-1 system.*[5]

---

[5] Task Force on Optimal Public Safety Answering Point Architecture*, Working Group 2 Report: Optimal 9-1-1 Service Architecture*, (December 10, 2015), Federal Communications Commission, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG2_FINAL_Report-121015.pdf.

As each 911 authority deploys NG911, it will develop the plan that is best for its jurisdiction given the respective environment and operations. A framework for evaluation/assessment that can be used in this diverse environment is needed and does not exist. Therefore, assessments of where states or local entities are in their deployments are not based on any specific and agreed-upon architecture framework.

Several frameworks and models were reviewed to best document the current status of NG911 and to prepare for developing the NG911 cost study. One framework was produced by the Standards Coordinating Council (SCC).

The SCC is developing and encouraging the development of standards and frameworks to improve the sharing of information related to public safety and national security in the Information Sharing Environment (ISE). The SCC developed the ISE Information Interoperability Framework (I2F)[6] as a part of its Project Interoperability.

> *The I2F is a national architecture framework designed to support information sharing for the public safety and national security missions across all levels of government – federal, state, local, tribal, and territorial.*[7]

Based on the nature of the public safety data and applications, the NG911 system will need to integrate with other public safety and national security systems to fully carry out the next generation vision and a nationally integrated and robust public safety communications network. The ISE I2F provides a common framework for achieving interoperability with these other systems. The Project Interoperability framework uses an Office of Management and Budget (OMB) document, Federal Enterprise Architecture Framework (FEAF), as a reference. A detailed description of the framework is included in Appendix A. The ISE I2F uses domains to define the systems and improve interoperability. The domains used are found in Figure 8 below.

---

[6] "ISE Information Interoperability Framework," Information Sharing Environment, May 2014, https://www.ise.gov/resources/document-library/ise-information-interoperability-framework.

[7] "Project Interoperability: A Start-Up Guide to Info Sharing," Project Interoperability, accessed September 15, 2017, http://project-interoperability.github.io/, paragraph 5.
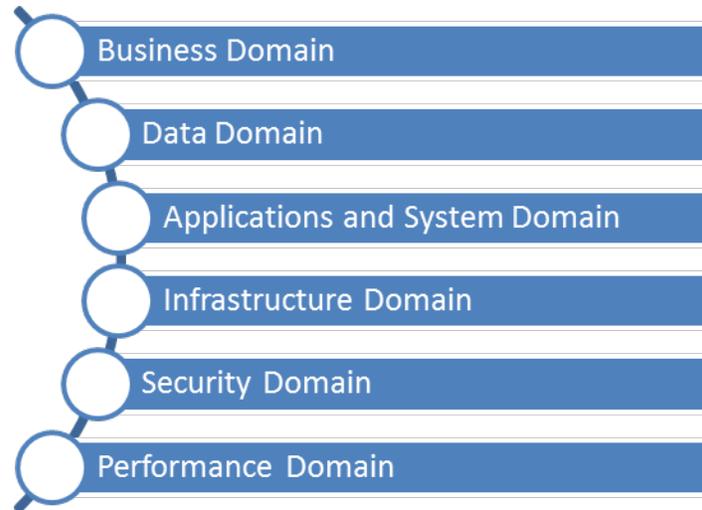
Figure 5: ISE I2F Domains

This framework model was adopted to provide further granularity in measuring the maturity of NG911 implementation across the United States.

2.3. NG911 Maturity Model

NG911 is an enterprise solution that will result in a nationwide system of systems that must share a common approach and be interoperable. The Team developed the NG911 Maturity Model to be used throughout the NG911 Cost Study project. The model was briefed to a broad audience of 911 professionals at conferences, professional organizations, and FCC working groups.

The NG911 Maturity Model uses the following components:
- NG911 Maturity Stages – Time frames of the NG911 transition
  - Legacy
  - Foundational
  - Transitional
  - Intermediate
  - End State
- NG911 Framework – Various functions and systems that are transitional steps or required for NG911
  - Domains – Major areas of focus
    - Business
    - Data
    - Applications and Systems
    - Infrastructure
    - Security

- Operations/Performance
  - Functional components – Specific functional or operational components of NG911 that are performed within the domain
  - Elements – Subset of functional components that are specific actions implemented, or systems deployed within a specific stage

2.3.1. *NG911 Maturity Stages*

The implementation of NG911 is a complex, phased process that may have multiple stages and multiple ways for a state to migrate to NG911. The process often is referred to as a journey and, as with any journey, there will be moments of rest, roadblocks, and strategic routes to reach the end destination. Since the 2009 Cost Value Risk Analysis report developed during the NG911 Initiative,[8] states/territories, regions, and PSAPs have moved forward with NG911 technologies.

The NG911 framework of domains, components, and elements is combined with a set of maturity stages to create the NG911 Maturity Model, which provides a series of common implementation stages. Each stage has a measurable, defined set of criteria for each aspect of an NG911 program. Each element of the NG911 components will reside in one or more stages to measure the maturity of NG911. Each component is independent of the others.

A PSAP, region, or state may be in more than one stage at any one time. For example, a PSAP may have IP-capable call-handling equipment in the Intermediate stage, while having Legacy call delivery. The NG911 Maturity Model measures the stage for each functional component, such as an ESInet or the development of GIS data. The NG911 Maturity Model provides a method of measuring progress for each specific component by assessing each element's stage.

The NG911 Maturity Model is in no way a roadmap; not every transitional stage is needed in every implementation. Adopters may choose to skip transitional stages based on their plans and the availability of services. The stages of the NG911 Maturity Model are defined below.

2.3.1.1. *Legacy*

The Legacy stage is characterized as the point in time where 911 services are provided by the traditional incumbent local exchange carrier (ILEC) with circuit-switched infrastructure and ALI circuits. Planning for NG911 has yet to occur and technology serving the PSAP provides no advanced feature functionality.

---

[8] U.S. Department of Transportation, Next Generation 9-1-1 (NG9-1-1) System Initiative Final Analysis of Cost, Value, and Risk, (March 5, 2009), https://ntl.bts.gov/lib/35000/35600/35650/USDOT_NG911_4-A2_FINAL_FinalCostValueRiskAnalysis_v1-0.pdf.

2.3.1.2. *Foundational*

As the name implies, the Foundational stage is where the groundwork and planning for NG911 implementation is initiated. NG911 feasibility studies are performed; governance, operational, and technical planning occurs; data preparation commences; and IP networks may be implemented. NG911 systems are not yet operational and system procurement is either planned or underway.

2.3.1.3. *Transitional*

The Transitional stage is the tipping point where services have migrated partially from the legacy environment and 911 services are enabled by an IP infrastructure. This marks the first stage where NG911 call-routing services are implemented. The ESInet is in place and delivering calls and location data. At this point, a governance model has been established and a detailed NG911 roadmap will be developed.

2.3.1.4. *Intermediate*

The Intermediate stage enhances the infrastructure and applications to incorporate advanced call- and data-delivery interfaces. Business and performance elements are maturing and are reviewed in regular intervals to optimize operations.

2.3.1.5. *End State*

The End State is the stage where NG911 standards-based systems are in place from call origination to call handling. ESInets are interconnected and the call continuum enables PSAPs to deliver rich data to first responders in the field.

The end goal of a nationwide NG911 system is that the nation's 911 system is fully interoperable with well-established policies and procedures to support operations. Early adopters of NG911 technologies may be on their third or fourth generation of core systems.

2.3.2. NG911 Framework Domains

The NG911 framework allows data from various entities to be gathered and reported in a more consistent and useable manner. Even as jurisdictions deploy different portions of the NG911 systems in different order, this framework may be used to measure the progress not only for this cost study project, but also well into the future as implementation of NG911 rolls out nationwide.

Next Generation 911 Maturity Model

Figure 6: NG911 Maturity Model

The framework consists of six domains. Each domain is divided into functional components. A functional component is a specific functional or operational component of an NG911 system that is performed within the domain. Each functional component has one or more elements that, when implemented, are indicators of the NG911 maturity level in that functional component. These domains are defined below.

2.3.2.1.   *Business Domain*

The Business Domain consists of those planning and procurement activities that must take place to lay the groundwork for a transition to NG911.

2.3.2.2. *Data Domain*

The Data Domain captures the data management responsibilities of PSAPs, regions, tribes, states, and national-level authorities as they prepare for and implement NG911. This domain includes a shift from tabular location data to full dependency on GIS data for the verification of caller location and routing of 911 calls.

2.3.2.3. *Applications and Systems Domain*

The Applications and Systems Domain describes the applications, systems, and other core functions of NG911 systems.

2.3.2.4. *Infrastructure Domain*

The Infrastructure Domain describes the infrastructure elements that interconnect the NGCS of the Applications and Systems Domain.

2.3.2.5. *Security Domain*

The Security Domain encompasses all cybersecurity and physical security technology and operations, including the network, facility, and personnel security associated with the implementation of NG911 services. Specifically, this domain focuses on the systems and applications required to develop a security posture appropriate for each stage of the NG911 Maturity Model.

2.3.2.6. *Operations/Performance Domain*

The Operations/Performance Domain describes the policies, procedures, and programs that are needed to effectively operate NG911 systems.

Appendix B identifies the detailed functional and technical requirements, as well as the standards, specifications, and best practices for each element and functional component of the NG911 Maturity Model.

2.4.   Analysis of NG911

There is little dispute that the nation's 911 emergency communications systems require a transition from outdated and obsolete analog technologies to current digital technologies that will support the diverse ways in which consumers communicate. Implementation of advanced communications services will provide significant benefits and will result in improved service delivery for the public and first responders.

The acknowledged benefits of rapid implementation of NG911 are:

- **Enhance flexibility, resiliency and survivability of the nation's 911 system**
  A coordinated approach and sufficiently funded NG911 transition will take advantage of the opportunities provided by NG911 technologies to assist public safety agencies in efficiently managing limited resources. The result is improved system flexibility, survivability assurances, and integral resiliency in 911 to allow for more nimble and responsive systems and more effective and robust services.

- **Increase compatibility with related emerging communication trends**
  Text and multimedia applications represent the bulk of communications for many Americans today, especially the younger generations and the deaf-and-hard-of-hearing community. Consumers expect and assume that emergency calls to 911 already support these modes of communications. The benefit of implementation of NG911 services will be increased compatibility with current and emerging technologies, and increased public confidence in the nation's 911 system.

- **Leverage technological opportunities and increase data-sharing potential to improve access to and response of emergency services.**
  Employing the technological advances readily available in today's communications marketplace will increase the public's access to emergency response services and the 911 center's opportunity to provide additional data and information for improved response capabilities, enhanced situational awareness and greater responder safety.

- **Enhance coordinated deployment and improved functionality and first responder interoperability.**
  A nationwide, coordinated approach to implementing NG911 will help to avoid fragmentation and disparity in service across the country. Nationwide implementation will save time and money, and improve functionality and interoperability for first responders. It also will provide enhanced services to the public for both individual incidents and large-scale incidents, as well as natural/manmade disaster response.

- **Decrease costs of operating parallel 911 systems**
  Coordination and nationwide deployment of NG911 services will increase efficiencies, and reduce the long-term cost problem of operating dual systems for a prolonged time period. Virtualization, interoperability, and convergence of applications will enable public safety agencies to access shared applications through common interfaces, thus increasing flexibility and reducing costs. The result not only is greater efficiencies and lower costs, but optimization of investments in systems, maintenance, technology, and staff resources while increasing services.

- **Reduce the risk of security vulnerabilities and improve emergency services reliability**
  NG911 promotes increased linkages and interconnectivity among 911 centers, enabling a robust redundancy and resiliency in the event of natural disasters or individual 911 center failures. Security vulnerabilities are reduced and denial of service events are minimized. Transition to a more resilient and robust network further reduces risks and threats associated with legacy vulnerabilities.

- **Improve emergency response and coordination**
  Implementing NG911 services brings considerably more information into the PSAP, which enables the PSAP to provide greater protection of public safety personnel, better emergency response, and enhanced situational awareness. This is accomplished through improved call processing, call routing, and service delivery to effect faster response times; dynamic and flexible network routing to mitigate outages; and an overall reduction in vulnerabilities—all of which leads to improved outcomes for the public. The result is greater opportunities to improve emergency response and save lives.

The benefits of NG911 undoubtedly will improve emergency communications and response in our nation. Consequently, there are risks associated with not implementing NG911 or even delaying implementation. A failure to act in a timely, coordinated, and effective manner will result in a variety of negative consequences; NG911 implementation will cost more, take longer, and be less efficient and effective.

The risks of inaction or delayed implementation include:

- **Inaction will prolong nationwide deployment and delay benefits of NG911 applications**
  An uncoordinated, underfunded or unfunded transition to NG911 will take years—many years and likely more than a decade, with many public safety agencies deferring deployment due to resource limitations. Indeed, it may never happen in some communities. The transition could take as long (or longer) than the Wireless Phase II transition, which was similarly sporadic and uncoordinated, and created pockets of disparate service levels across the country. The result of delayed or nonexistent implementation in areas of the country will be inconsistent service levels and underutilized capabilities until all public safety agencies have transitioned to end state NG911.

- **Inaction will risk incompatibility with emerging communications trends**
  Communications preferences of U.S. consumers have evolved dramatically in recent years, with relatively few willing to accept voice-only services. Text and multimedia applications represent the bulk of communications for many Americans today, especially the younger generations and the deaf-and-hard-of-hearing community. Consumers expect that emergency calls to 911 will support these modes of communications. The result of inaction or slowed implementation of NG911 will be a lack of confidence in the nation's 911 system and underserving large communities of the public. The same holds true for public safety responders, many of whom already use multimedia services or soon will with the launch of the NPSBN.

- **Inaction will create technological obsolescence and present service risks**
  The commercial marketplace already largely announced their plans to make the technology transition that clearly faces the 911 community, migrating from outdated technologies to the advanced IP-based technologies that drive today's communications services. Network providers publicly have announced that they are seeking to retire legacy infrastructure as quickly as possible. Continued reliance on this outdated infrastructure will render 911 systems obsolete and isolated technologically. The result will be significantly higher costs required to continue to support outmoded systems, and higher risk of outages and service failures.

- **Inaction will result in "patchwork" deployment, limit interoperability and risk uncoordinated implementation**
  Without a focused effort and adequate cost understanding, NG911 largely will be deployed on an uncoordinated basis. States are being encouraged to undertake coordinated efforts, but some will not or are not authorized to do so. Thus, many local agencies will have to bear the responsibility of deciding when and how to make the transition, and how to fund it. The result will be a patchwork system with individual agencies having widely varied capabilities and limited interoperability with neighboring agencies, regions or border communities.

- **Inaction will risk increasing the costs of operating 911 systems**
  During the transition to NG911, public safety agencies will have to pay the implementation and operations costs of NG911 while also paying for the continued support and operation of legacy systems. Therefore, an extended transition period will result in substantially greater costs to state and local agencies. In addition, funding the NG911 transition as a series of uncoordinated local programs will drive cost inefficiencies and increase the overall cost burden on state and local 911 authorities.

- **Inaction will risk security vulnerabilities and reduce reliability**
  A fragmented and prolonged transition to NG911 will make it more difficult to maintain the reliability, and protect the security, of the 911 system, cyber or otherwise, and will delay implementation of more-robust reliability and security measures that will be present in the mature NG911 environment. The result is higher risk for security breaches and increased vulnerabilities of the nation's critical infrastructure.

- **Inaction will result in missed opportunities to improve emergency response, and risk the responder's ability to positively impact outcomes**
  The emergence of advanced broadband communications can put much more powerful capabilities in the hands of first responders. Without NG911, however, first responders will not be able to receive the enhanced information available from the public through text, video, and data access to the 911 system. The result will be a less effective broadband communication system and less-than-optimal response to the public's call for help.[9]

The status of 911 services impact governance, technology, operations, and funding in every emergency communications center, in every community, and in every state and territory of this country. How NG911 is implemented, how it is funded and whether it moves forward in a coordinated way has wide-reaching implications for public and private life in America.

2.4.1. *Functional Needs Community Concerns*

Barriers to special populations such as the deaf-and-hard-of-hearing community are becoming more widely understood and their concerns more readily embraced. The Department of Justice (DOJ) filed comments in the FCC's text-to-9-1-1 rulemaking proceeding stating that "in fulfillment of their existing obligation to provide effective communication under title II of the ADA, PSAPs must accept a call from a person with a hearing or speech disability that originates as an SMS call, but reaches the PSAP as a TTY call."[10] While text-to-911 capabilities are not necessarily an NG911 implementation issue as an interim solution is available prior to full implementation of NG911, the full function and benefits of text-to-911 only can be realized with NG911 implementation.

---

[9] "Benefits and Consequences of NG911 Implementation," http://www.ng911now.org/#about.

[10] U.S. Department of Justice, *Comments to Federal Communications Commission's Further Notice of Proposed Rulemaking*, *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment,* https://ecfsapi.fcc.gov/file/7022129201.pdf, paragraph 4.

Title II of the Americans with Disabilities Act (ADA) applies to state and local government entities and, in Subtitle A, protects qualified individuals with disabilities from discrimination on the basis of disability in services, programs, and activities provided by state and local governments.[11]

Title II regulation requires that public entities—including 911 centers—"that communicate by telephone with applicants and beneficiaries use TTYs or another equally effective telecommunications system to communicate with individuals who are deaf or hard of hearing, or have speech impairments—unless the entity can demonstrate that doing so would result in a fundamental alteration in the nature of a service, program, or activity, or in undue financial and administrative burdens."[12]

The electronic filing goes on to state: "The Department recognizes that many individuals with disabilities now use wireless text devices and the Internet, rather than analog-based TTYs, as their primary modes of telecommunications. Our understanding of the FNPRM is that PSAPs may use existing TTY-based telecommunications systems to process text (SMS)-to-TTY calls. Therefore, in fulfillment of their existing obligation to provide effective communication under title II of the ADA, PSAPs must accept a call from a person with a hearing or speech disability that originates as an SMS call, but reaches the PSAP as a TTY call."[13] If Title II entities choose to accept SMS calls from individuals with disabilities through an IP system, the Department would consider that as using an equally effective telecommunications system; thus, such entities would be in compliance with §35.161(a) of the Act.

Although both the FCC and the DOJ clearly promote text-to-9-1-1 services implementation nationwide, there is nothing in the FCC rulemaking or the DOJ's currently published interpretation of statutes that requires an entity to accept text messages from hearing- and/or speech-impaired persons, or other persons without disabilities. However, if an agency is implementing IP technology to receive 9-1-1 calls from the population it serves, the Department is clear that hearing- and speech-impaired persons should be afforded equal access using equal services as a fulfillment of their obligation under the law. At the time of this publication, the DOJ has an open rulemaking on NG911 obligations for PSAPs, which may result in additional guidance in the future.

---

[11] U.S. Department of Justice, *Title II Highlights,* (August 29, 2002), *Overview of Requirements,* https://www.ada.gov/t2hlt95.htm.

[12] U.S. Department of Justice, *Comments to Federal Communications Commission's Further Notice of Proposed Rulemaking*, *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment,* https://ecfsapi.fcc.gov/file/7022129201.pdf, paragraph 3.

[13] Ibid., paragraph 4.

2.4.2. Governance – The Need for National Guidance and Statewide Coordination

The implementation of NG911 nationwide represents a transformational change. The history of 911 has been plagued with lesser transitions and incremental updates since its inception. While transitions and updates traditionally have been accomplished at the local or regional level, NG911 transformational change requires all levels—up to and including the state and nationwide levels— as well as local non-911 entities, to work collaboratively.

In addition to the normal transition to new technologies, NG911 technologies are shared by and interconnected to other jurisdictions. This sharing of resources, and interconnection, on such a large scale, is still new to a public safety sector that has been siloed and jurisdictionally based for so long. The need to adopt new policies and procedures, as well as to interoperate with various new systems, will transform the 911 system of the future. New governance concepts that permit interstate collaborations and joint public/private partnerships, and which encourage flexible oversight and management by non-governmental entities, will be the only way the full benefits and flexibility of NG911 will be realized.

The NG911 network will be a system of systems that requires detailed coordination for connection between the systems, and cooperative agreements to share data between the entities at higher and higher levels within the government spectrum will be required. Because the vision for NG911 is a mesh of integrated networks and systems that ultimately spread across the country to theoretically interconnect all emergency communications systems from coast to coast and border to border, the need for governments to be willing to participate in agreements with neighboring states becomes more significant and necessary. Interstate interconnection agreements do not currently exist in very many situations, as states heretofore have not had the need to extensively collaborate on critical issues. Waterway management and highway infrastructure may be the exception and much can be learned from those collaborations.

Overarching the state integration is the need for nationwide guidance. To facilitate a nationwide transition to NG911, it will be necessary to have some level of nationwide governance. There will be a need for states to interconnect networks to be able to transfer calls, synchronize GIS files, and share data. Nationwide governance does not mean a federal agency must operate 911, but there needs to be nationwide coordination. Just as the statewide plans for NG911 will assist the entities within a state to be able to interconnect their systems to each other, the state-to-state collaboration needed to interconnect state systems is also critical to the success of NG911. A nationwide vision and guidance is needed to encourage state interconnectivity to achieve the goal of ubiquitous NG911. Key elements of this initiative include a gap analysis and a nationwide NG911 plan.

2.4.3. Technology – Assessment of Architectural Characteristics and Limitations

The migration to NG911 will require service providers to make significant changes in the OSE. Service providers must migrate from the current TDM call-delivery environment to SIP delivery over IP networks. Service providers are moving slowly from the legacy Public Switched Telephone Network (PSTN) Class 5 switches to IP-based softswitches using SIP to deliver calls. During the transition period from legacy 911 to NG911, the service providers will have to install legacy network gateways to translate the TDM circuits to SIP for delivery across the ESInet. Once the transition to the NG911 end state is complete, the gateway functionality will be decommissioned, though the physical devices may remain in service to perform other vital network functions. Interim steps such as this that employ technology for a limited period of time are costly and resource-intensive.

One major change that NG911 brings with it is how the delivery of the 911 caller's location information is handled. The location information currently is delivered by an ALI bid to a static database after the call is answered by the PSAP. In the NG911 environment, the location information is delivered to the PSAP in the SIP message headers along with the call, although the location information is more dynamic and still can be updated by the call-taker during the call. The service providers will be required to develop and manage their own LIS to provide the location information in the initial call delivery, and to provide updates throughout the call process.

As the PSTN migrates to an IP-based system, outside call centers such as poison control, language lines, N-1-1, and others will require upgrades to their systems and infrastructure in order to handle SIP calls. In the transition period, gateways may be required to connect these outside call centers to the PSAP network.

2.4.4. Funding – A National View

In the U.S., the provisioning of 911 service traditionally has been focused at the local level. Each agency would contract with its local provider for the level of 911 service that was available. Over the years, as the industry matured, more states and agencies developed parameters, rules and definitions, as well as funding mechanisms, that have left the scope of 911 service not clearly agreed upon. Many states define 911 as receiving a call from the public networks, but do not include the dispatch function in their definition, even though the function is performed by the PSAP. In some cases, if it is not included in the definition, it is not eligible for funding. Other states include some of the dispatching equipment, but not staffing. Other states will allow all PSAP costs and some even the responders' communications equipment. The varied level of methods used to define PSAP eligible costs, the mechanisms to collect funding for 911 service, and the lack of comprehensive data collection regarding funding all have impacted the ability to generate a clear picture of what is currently spent on 911 operations that is valid and comparable from state to state.

2.5.   Operations – Variable Access to Broadband

Although many consider broadband to be widely deployed, there are areas in the country where it is either not deployed, or is deployed but with bandwidth limitations, especially in rural areas and on tribal lands.[14] The limitations may be due to distance, loop quality, or other factors.[15] While Figure 10 below illustrates that 80 percent of the country or more is covered by broadband, data on PSAP access to the necessary bandwidth for processing NG911 data has not been gathered on a nationwide basis.
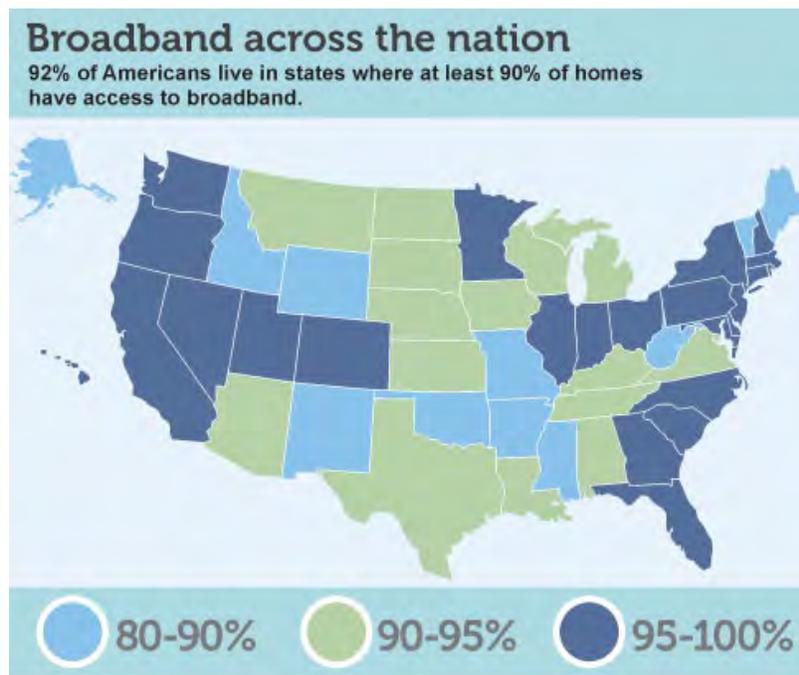
Figure 7: Nationwide Broadband Deployment (Source US Telecom[16])

The PSAP-to-responder network transfers information from the PSAP to responders in the field. Migrating to NG911 will give PSAPs the ability to natively handle SIP-based voice, text, multimedia, machine-to-machine, and other IP-network-enabled call types.

The any-to-any nature of IP networks enhances the disaster recovery options available to 911 centers. Implementing call-handling systems in a hosted model (e.g., collocated in data centers

---

[14] "2016 Broadband Progress Report," Federal Communications Commission, January 29, 2016, https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report.

[15] "Broadband Deployment," USTelecom, 2017, http://www.ustelecom.org/issues/using-broadband/broadband-deployment.

[16] Ibid.

with the NGCS) enables PSAPs to deploy resources anywhere they have access to a secure broadband connection. Using a specially configured and secured laptop, personnel can log into the hosted call-handling system and take calls as if they were in their normal PSAP.

The implementation of the NG911 environment and IP-based networks enables native integration of new devices and services into the NG911 system. Examples include, but are not limited to, alarms, sensors, and other IP-based devices and services that may be developed in the future. The move to NG911 is the first step in getting supplemental data to emergency responders. Appendix C – Detailed NG911 Analysis contains additional information on the limitations and feasibility of NG911.

This page is intentionally left blank.

3. CURRENT ENVIRONMENT

For this report, more than 15 different definitions of NG911 were collected from reputable sources. The differences in terminology are as minute as a single word or element, and as vast as the entire concept of what is included in the definition of NG911. The mere fact that so many definitions exist makes it difficult to establish exactly where each 911 authority is regarding implementation, and illustrates the challenges in assessing readiness. The NG911 Maturity Model was developed to focus on the required functions of NG911 rather than the names used to describe specific NG911 components, in order to address conflicts among definitions.

In addition, the data available for analysis of the current status of NG911 is self-reported to the National 911 Program or the FCC via the *2016 National 911 Progress Report* (including responses from 46 states and territories) and the FCC's *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*. This data is based on the submitter's perception or understanding of the services or systems implemented or in implementation as of the end of calendar year 2015. This impacted the accuracy of this data and SMEs were engaged to attempt to qualify this data. Depending on the definition used, or assessment consulted, data inconsistencies may have impacted the analysis.

One thing that is clearly understood is that all the elements of NG911 must be present and functioning in order for NG911 to be considered fully implemented. With this in mind, and based on the analysis conducted, there are no states in the end state of NG911 implementation.

To track progress toward NG911, a survey question was added to the 2015 survey for the *2016 National 911 Progress Report* regarding the number of ESInets in each state. Many states now are developing either statewide or regional ESInets that PSAPs and 911 authorities can access. Data element 3.2.4.3 in the Progress Report presents information on ESInets by state.[17]

In many cases, states are implementing NG911 networks incrementally, as circumstances enable their ability to plan for, fund, and carry out deployment. The purpose of the National Profile Database data collection was to identify states that are at least advancing NG911 capabilities and components. It should be noted that data self-reported by 911 authorities without a single universally accepted definition of NG911 may not permit confident conclusions. However, ESInets—the implementation progress of which is presented in Table 5 below—are one of the most important initial elements for measuring progress toward NG911. It should be noted that ESInets are initiated in the Foundational Stage and their implementation continues in all stages to the End State stage.

---

[17] National 911 Program, *2016 National 911 Progress Report,* (December 2016), https://www.911.gov/pdf/National-911-Program-2016-ProfileDatabaseProgressReport-120516.pdf.

A review of the current status of NG911 implementation used in this study readily illustrates the various stages of readiness. Progress is exceedingly slow. Over the previous three years, the numbers in each of these categories only moved by small amounts.

Table 3: States Reporting NG911 ESInet Progress

Deployment Element	2013	2014	2015	+/- Change in States Reporting	% of the States
Statewide NG911 Plan Adopted	15 of 39 states reporting	19 of 42	20 of 46	+5	40%
Statewide Request for Proposals Released	13 of 36	18 of 42	19 of 46	+6	38%
State Contract Has Been Awarded	13 of 29	16 of 42	19 of 46	+6	38%
Statewide Installation and Testing	9 of 30	11 of 42	18 of 46	+9	36%

The NG911 current status shows that the Business Domain is well into the early majority, as defined by the Innovation Adoption Lifecycle, with 26.4 percent of the nation beginning to implement NG911. The next largest domain is Applications and Systems, which is also into the early majority stage, with 20.8 percent of the nation beginning to implement NG911. Additional implementations in the Infrastructure, Data, and Security Domains are in the early adopters, but have begun. The laggard seems to be the Operations/Performance Domain, which is understandable as many of the systems are still in the implementation or early service life.

Table 4: NG911 Current Status

	Legacy	Foundational	Transitional	Intermediate	End State
Business Domain	73.6%	16.4%	2.9%	7.1%	
Data Domain	89.0%		8.2%	2.8%	
Applications and Systems Domain	79.2%	10.0%	1.0%	9.8%	
Infrastructure Domain	88.2%	10.2%		1.6%	
Security Domain	86.9%	7.1%	6.0%		
Operations/ Performance Domain	98.0%	2.0%			

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

Just as the definition of NG911 is varied, the manner in which legacy 911 service has been implemented throughout the country is equally varied, because such service traditionally has been jurisdictionally siloed. This diversity of implementations and local preference has given rise to a strong desire to continue to do things in a local way. In some cases, state statute assigns decision-making for 911 operations to the lowest level of local government, to ensure that the response requirements are kept local.

There are many more ways to implement NG911 than there were to implement basic 911 service so many years ago. However, the driving need to interoperate has challenged and compromised the previously held notion that it was essential to make decisions at a local level, and only those local decisions fully contemplated the needs of the community. However, more and more forward-thinking 911 authorities now recognize the importance of integrating, interconnecting, and sharing networks and other resources with neighboring systems to benefit from the efficiencies provided by successful NG911 implementations. The 911 leaders of today who embrace technology as a critical and essential tool in the emergency communications ecosystem understand the need for data—the importance of "big" data, the value of immediate data, and the power of shared data.

NG911 and the promise of its flexibility and capabilities to address so many of the restrictions and problems that have plagued 911 operations can encourage a more free and unencumbered vision regarding the possibilities for 911 effectiveness. Much more could be accomplished if public safety and government leaders do not restrict themselves with the old ways of doing things, the constraints of challenging funding models, the siloed governance mindset, or policies that stymie vision.

4.   COST ANALYSIS FRAMEWORK

The overall approach to estimating the LCCE of nationwide implementation of NG911 systems is illustrated in Figure 11 below. This overall approach follows the U.S. Government Accountability Office (GAO) Cost Estimating and Assessment Guide (GAO's LCCE Development Process) and the Federal Highway Administration (FHWA) Life-Cycle Analysis Primer Guidelines.
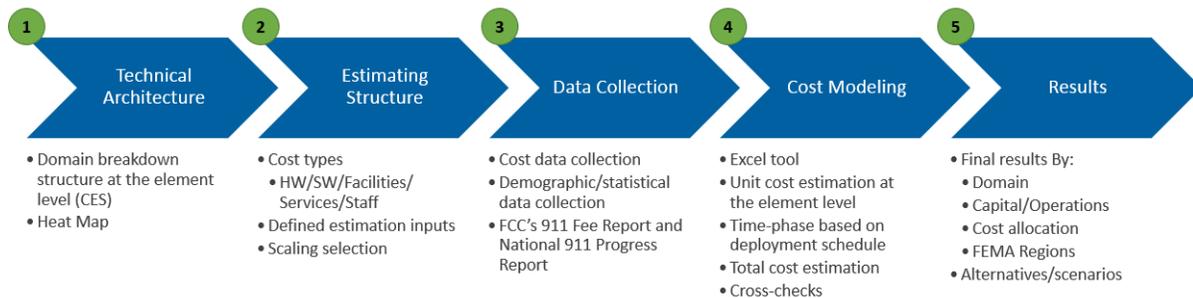
Figure 8: Overall Cost Estimation Approach

The cost study was developed based upon the NG911 Maturity Model detailed in the NG911 functional requirements, technical requirements, and specifications. This technical architecture was used to create the Cost Element Structure (CES) used in the estimate with the following hierarchy: domain, functional component, and element. This CES was used to identify cost categories and scaling factors associated with each element within the NG911 Maturity Model and define specific assumptions related to each data input. Each element within the NG911 Maturity Model is estimated in terms of five cost types:

- Hardware – workstations, call-routing equipment, routers, servers, etc.
- Software – geospatial routing software, CAD, etc.
- Staff – government and contractor labor for policy, governance, security, etc.
- Facilities – data center facilities, NOCs/SOCs, office space, etc.
- Services – GIS data management services, broadband connectivity, etc.

The NG911 current status assessment contained in Section 3 of this report represents the estimated portion of the nationwide population that is covered by systems that meet the definitions of the NG911 Maturity Model for the various functional components and stages. The NG911 current status was an essential input to the NG911 cost model.

Microsoft Excel was the primary tool used for modeling this cost study. The model documents data sources and allows traceability of the inputs, calculations, and modeling assumptions for document verification and validation. The model is a build-up/bottom-up estimate in which costs are estimated at the element level and are aggregated up to functional component and domain level costs.

4.1.   Data Sources

Two major types of data were collected for this study: statistical and cost.

Statistical Data was collected from publicly available sources such as:
- U.S. Census and FHWA – collected data examples include population, urban and rural area, land use, density, number of counties, etc.
- FCC *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, *2016 National 911 Progress Report* (including responses from 46 states and territories),[18] and FCC Voice Telephone Services report (2015)[19] – collected data examples include number of primary and secondary PSAPs, total number of calls/texts to 911, wireline and mobile service providers, etc.

Cost Data was collected from a variety of sources such as:
- Publicly available NG911 actual or estimated cost data and cost studies – most preferred source of cost data collection.
- General Services Administration (GSA) Advantage[20] and other technology solution providers such as CDW[21] – specified hardware suites and services
- SME inputs – regional level costs, level of effort, and staffing categories, etc.
- Manufacturers' recommended prices

4.2.   Period of Analysis and Inflation Assumptions

Inflation rate accounts for the sustained increase in the general level of prices in the economy. Historical cost data collected for this study are escalated to adjust for inflation to estimate future costs. Previous year collected costs are normalized to a base year to account for historical inflation. The estimating approach using these 2017 constant year values is summarized below.

---

[18] National 911 Program, *2016 National 911 Progress Report,* (December 2016), https://www.911.gov/pdf/National-911-Program-2016-ProfileDatabaseProgressReport-120516.pdf.

[19] "Voice Telephone Services Report," Federal Communications Commission, June 30, 2016, https://www.fcc.gov/voice-telephone-services-report.

[20] "Advantage Online Shopping," U.S. General Services Administration, https://www.gsaadvantage.gov/advantage/main/home.do.

[21] CDW, 2017, https://www.cdw.com/.

- All historical data are escalated to the 2017 base year
- Unit costs are estimated in this base year for the purpose of developing CERs and other estimating methodologies
- Estimated total costs are spread using time-phasing methodologies based on the implementation schedule resulting in an obligation profile
- Base year costs in each time period (year of analysis) are escalated to then-year dollars using that year's proper inflation index
- The total ten-year cumulative costs presented in this report are all inflation-adjusted dollars for a ten-year period of analysis

4.3. Geographical Assumptions

To determine the cost distribution of planning, acquisition, implementation, and maintenance of NG911 systems by geographic areas and population size, FEMA's ten multistate regions[22] were utilized in the cost model analysis, as illustrated in Figure 12 below. It is important to note that each FEMA region has unique factors and characteristics regarding NG911 readiness (NG911 current status), population, number and size of PSAPs, and NG911 OSPs, which contributes to their unique costs.

---

[22] "Regional Contact Information," Federal Emergency Management Agency,
https://emilms.fema.gov/IS101c/DEP0101150text.htm.
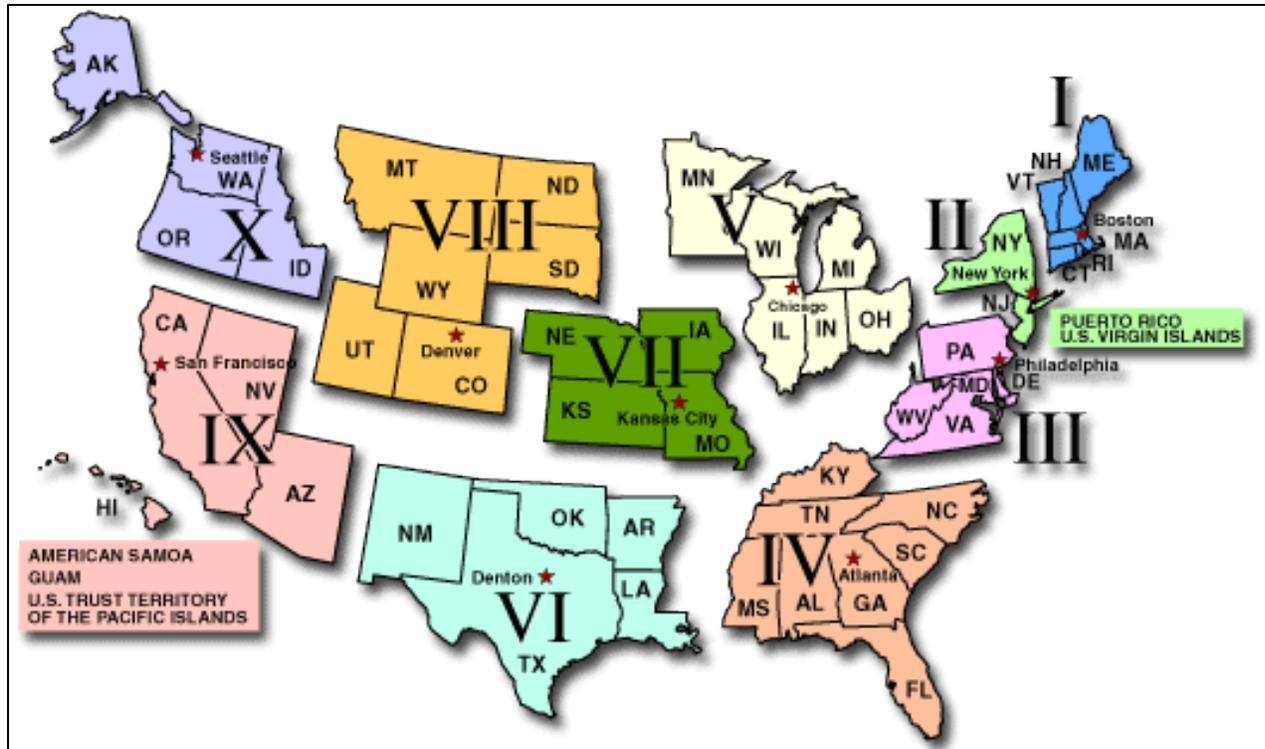
Figure 9: FEMA Regional Map[23]

4.4.   Scaling Factor Assumptions

This study divided the nation into geographical regions/municipalities (urban, rural, etc.)—using U.S. Census data and the FEMA regions—to accommodate regional variances in NG911 system requirements. Scaling factors were used to extrapolate the estimated unit costs to a nationwide level total cost for each geographical region/municipality. As this study analyzes a varying range of costs—from planning to acquisition and implementation to maintenance—using a single scaling parameter was deemed impractical. Therefore, depending on the characteristics of each element within a domain, an appropriate scaling factor was identified by SMEs and used as a multiplier. Some of the scaling factors were derived from available statistical data sources while others were derived from SME regional inputs. Some examples of scaling factors are listed in Table 7 below. Where each of the scaling factors is used is described within Appendix D – Maturity Model Assumptions and Data Sources.

---

[23] Ibid.

Table 5: Scaling Factor Examples

Scaling Factor	Source	Functional Area Example
Geographical regions – urban, rural, etc. (population/area/density)	U.S. Census	Various areas as well as extrapolating unknown values
Number and size of PSAPs (based on the number of positions)	FCC's *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges* and SME state-level input	Egress network, CPE, servers, workstations
Number of counties	U.S. Census	GIS location database management
Number and size of cores (based on the population served by the core)	SME state-level input	Data centers, NOC
Network bandwidth	SME input	Ingress, egress, ESInet fees
Number of service providers	*Voice Telephone Services* report (2015)	LNGs, selective router fees, trunks/circuits
Call volume	*2016 National 911 Progress Report*	Event logging, data analytics, quality assurance (QA), BCF
Level of effort	SME state-level input	Business and Operations Domains

4.5.   Operating Entity Allocation

Each element was identified with an operating entity allocation tag so that the costs could be identified as to where in the system of systems they may be allocated. However, this allocation may not directly relate to the entity that pays those costs. Allowable 911 costs vary across the nation as each state allocates the costs differently. The allocation entities used for this study were as follows, and used for subsequent cost summaries:

- Service Provider – These costs include location data and systems that would be needed for NG911. These OSP costs traditionally have been passed on to 911 users and are not directly paid for by the OSP.
- State – The cost study allocated costs such as planning and coordination of GIS data to the state. These may be paid by the PSAPs or a regional entity within a state.
- Next Generation Core Services – The cost study included NGCS hardware, software, and services. These may be paid by the PSAPs, a state, or a regional entity within a state.

- PSAP – Such costs are those directly related to systems within the PSAP.
- Federal – The system costs for nationwide elements were tagged as federal costs. These costs are not necessarily allocated to a federal agency, but are nationwide in scope.

4.6.   Ground Rules and Assumptions

The purpose of establishing ground rules and assumptions (GR&As) is to provide visibility into the cost estimation methodology used to develop the LCCE for the nationwide planning, acquisition, implementation, and sustainment of NG911 systems, within certain parameters and boundaries. The GR&As for this estimate represent overarching cost assumptions or even those leveraged within the NG911 Maturity Model analysis results.

Global assumptions outline a set of standards and parameters applied to the entire analysis and provide guidelines and boundaries for the cost model. However, more-in-depth assumptions and domain-specific assumptions for each functional component and element within the NG911 Maturity Model are included in Appendix D – Maturity Model Assumptions and Data Sources.

4.6.1. Global Assumptions

In general, cost estimates of this far-reaching nature are produced with limited information and specific data applicable to every jurisdiction. Therefore, estimates need to be clearly defined and bounded by constraints that make estimating possible. Such constraints are summarized in this section in terms of the global assumptions that define the cost estimate's scope. Due to the nature of the NG911 implementation process, there are inherently many unknowns when estimating the lifecycle costs of NG911 at the nationwide level. This section summarizes the comprehensive list of global assumptions that define the conditions upon which the cost estimate is based. It also provides a means for reconstruction of the cost estimate for future studies.

- This study produces a range of costs for the nationwide implementation of NG911. The range of costs is based on the assumptions identified in this section and Appendix C.
- Costs of operating and maintaining the currently fielded 911 systems (legacy or NG911) are outside the scope of this study. As a result, no costs have been identified for the legacy stage of the NG911 Maturity Model.
- Elements that apply to the nationwide level of NG911 operations are costed out for that entity as a whole and scaled for the nation.
- This study is not intended to be a technical guide for states as they build their infrastructure, or for which technologies or vendors to select.
- No specific vendor products are endorsed in this study. Instead, wherever possible, average costs are developed and used.

- Each element's transition is based on the previous stage and what it takes to progress. It is important to note that any individual geographical area may have different assumptions for the status of deployment to the NG911 end state.
- The NG911 Maturity Model included an end-to-end system of systems, from call entry into the NG911 system to the delivery of information to responders.
- While some components (e.g., public safety radio systems) of the emergency communications ecosystem—the public safety system of systems—are included in the NG911 Maturity Model, their associated costs may not be included within this cost analysis.[24]
  - o Specifically, OSE costs to update the respective networks were not included due to the many public statements concerning plans to update the networks and discontinue legacy services
  - o PSAP-to-responder costs were not included. This includes the current land mobile radio (LMR) systems in place, but also the costs to PSAPs of interconnecting to the NPSBN, given that the specifics of such interconnection are still in development and will depend on how a PSAP chooses to use FirstNet, which services are used and the services that first responders are using
  - o Federal agency PSAPs were not included in the cost study. Several departments mentioned that the "Purpose Statute" 31 USC § 1301(a) may impact their implementation of NG911 without proper appropriations. These PSAPs are expected to use their respective agencies' regular budgeting process. However, it is important to ensure that the agencies are supported by NGCS
- Specifications and standards (e.g., *Detailed Functional and Interface Specifications for the NENA i3 Solution*), identified in Appendix A – NG911 Architecture, are considered in the cost model. These specifications and standards are considered for products required for each individual transition as they are vetted for inclusion.
- For optimal organization at the national level, each state is assumed to have a single coordination entity for its NG911 network. For estimation purposes, a statewide coordination activity is included for each individual state. The level of authority of the coordinating entity varies currently from state to state, but 911 community experience from wireless and VoIP deployments has found some form of statewide coordination is a key to successful implementation.
- The NG911 Maturity Model is a framework that defines the technical requirements and system specifications of the NG911 enterprise solution. The framework's domains, functional components, and elements are used as the CES for this cost study. The complete

---

[24] There are other aspects of NG911 technology implementation that are driven by completely different factors. Only those costs that are incurred within, or between identified end points, are included to clearly demarcate the boundaries of inclusion. Primarily this is limited to specific communication networks between dispatchers and emergency responders.

CES hierarchy used in the cost estimation is included in Appendix D, Section D.8 – Reference Tables, Table D-35.

4.7. Public Safety Answering Point Assumptions

For the purpose of this study, the current number of PSAPs[25] (derived from the FCC's *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*) is considered sufficient to serve the population of the respective region/municipality. Therefore, evaluating this quantity with respect to a more optimal number of PSAPs in the end state is not analyzed in this study and is out of scope.

Due to the lack of detailed data on exact number of positions per PSAP in each region, the Team, in collaboration with SMEs, made assumptions about PSAP size distribution and number of positions per PSAP size. Four PSAP size categories—small, medium, large, and mega—have been identified by SMEs for this cost study. The national average PSAP sizes and their associated minimum, maximum, and most likely number of positions are summarized in Table 8 below.

Table 6: PSAP Distribution and Number of Positions

PSAP Size	% of Total PSAPs	Number of Positions per PSAP – Minimum	Number of Positions per PSAP – Maximum	Number of Positions per PSAP – Most Likely
Small	85% of non-mega PSAPs	2	6	3
Medium	12% of non-mega PSAPs	7	20	12
Large	3% of non-mega PSAPs	21	50	30
Mega	SME input[26]	51	200	100

The PSAP size distribution—as well as minimum, maximum, and most likely number of positions per PSAP—was established based on an analysis performed on publicly available or SME-experienced actual data from 13 different states, collected across the last ten years. Although PSAP size and actual number of positions in each location vary significantly throughout the U.S., the most likely number of positions per PSAP illustrated in Table 8 above was assumed as a national

---

[25] Derived from combining the latest available FCC's *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges* and the *2016 National 911 Progress Report*.

[26] SMEs reviewed the top 50 MSAs and identified the number of mega PSAPs currently in operation.

average and employed in the model. Using the current number of PSAPs, the assumed PSAP size distribution, and the most likely number of positions per PSAP, a total of approximately 30,000 workstations was calculated and used in the study. According to the Bureau of Labor Statistics, the total number of police, fire, and ambulance dispatchers in 2014 was 102,000.[27] This demonstrates roughly a 3.5 to 1 ratio of dispatchers to estimated PSAP positions, which was an accurate representation based on SME opinion, considering the 24-hour nature of PSAPs and staffing considerations due to that timing.

---

[27] "Occupational Outlook Handbook, Police, Fire, and Ambulance Dispatchers," U.S. Department of Labor, December 12, 2015, https://www.bls.gov/ooh/office-and-administrative-support/police-fire-and-ambulance-dispatchers.htm.

5.   COST ANALYSIS

The cost analysis focused on the most defensible implementation alternatives to provide a cost estimate of planning, acquisition, implementation, and sustaining NG911 systems for the entire U.S., including territories. The cost study leveraged an evaluation of current environment (i.e., NG911 Maturity Model current status) as well as a series of actual and estimated cost data from publicly and privately available sources.

The analysis is most useful in gaining an understanding of the actual cost categories required for each functional component within the NG911 Maturity Model, as well as a nationwide-level estimate based on the assumptions. Thus, while the estimates of total cost are dependent on the assumptions of projected implementation scenarios, and as such are uncertain (due to inherent uncertainty in any long-term predictions), all global assumptions are held constant for all FEMA regions. Therefore, by holding the global assumptions constant, it was possible to introduce state-level inputs and assumptions into the multistate areas, and to create unique and meaningful estimates.

The aggregation of multistate estimates, as well as nationwide-level cost requirements, resulted in total ten-year costs of NG911 systems. As a result, the analysis is most credible when looked at as the total nationwide NG911 cost, and is not intended to help determine individual state or locality costs.

It is important to note the aspects below that must be considered as the nationwide results are evaluated.

- The results include the additional NG911 costs to achieve the defined end state from the current status of each multistate area, and is not starting from the legacy stage for every area.
- The results exclude costs that an area has expended or is currently operating as components of an evolving, NG911-capable implementation.
- Any future technology enhancements and/or economy-of-scale applications can change the results drastically.
- Deviations from any of the implementation scenarios presented in this report can change the total cost.
- Actual start year and implementation path chosen by each area also can result in deviations from the total ten-year LCCE.

Sections 5.1.1 through 5.1.3 provide the cost estimate results to plan, acquire, and implement NG911 systems for the state, multistate, and service solution implementation scenarios, by operating entity allocations and domains.

For each area, as it achieves the desired end state, there is expected to be a period where both systems must operate to complete a break-in period and to retire legacy systems. After this period, states are expected to continue operating and maintaining their own expected NG911 functionality. The charts and tables in this section depict the complete deployment costs, but end with the second year after an area has reached its end state. Therefore, as each area reaches the NG911 end state, plus two years of dual-system operation, any further recurring or equipment refresh costs are excluded. Table 9 below summarizes the one-time and recurring deployment costs of the three scenarios. One-time costs can include equipment purchases, installation fees, or upfront fees. Recurring fees are usually monthly or annual fees for services, licensing, or maintenance.

As a result of the uncertainty analysis conducted at the end of this study, the final results shown for the scenarios appear to be conservative, expected to be in 85th percentile range. This means that the costs for these deployment scenarios should be lower 85 percent of the time. This analysis did not include cost risks, but a quantification of the uncertainty with respect to the estimating assumptions and inputs. Please see Appendix E, Section E.2 – Uncertainty Analysis for more information.

Table 7: NG911 Total Deployment Cost Estimation

Cost Type	State Implementation	Multistate Implementation	Service Solution
One-Time Cost	$3,022.3M	$2,898.8M	$599.3M
Recurring Cost	$7,508.1M	$6,606.5M	$12,115.3M
Total	**$10,530.4M**	**$9,505.3M**	**$12,714.6M**

The NG911 cost model used for the cost analysis calculates the deployment costs of a nationwide migration to the NG911 end state with systems based upon the functional requirements, technical requirements, and specifications developed for the cost study. Appendix E – Cost Analysis Detailed Results, contains the full ten-year LCCE study costs.

Figure 13 below shows the year-by-year costs of these deployment excursions for the three implementation scenarios. For the state and multistate scenarios, costs begin to decrease in years 8 and 9 as early-adopting regions and fast implementers have surpassed their end state by two years; the cost increases in year 10 represent the slow-adopting regions just reaching their first full year of operation. Meanwhile, the service-solution scenario shows a steady increase as regions begin implementation, and a decrease as the end state is achieved. Ongoing operational costs, represented by the dashed line, grow rapidly as the areas go from the deployment phase to ongoing operations, and are not included in the deployment costs from Table 9.
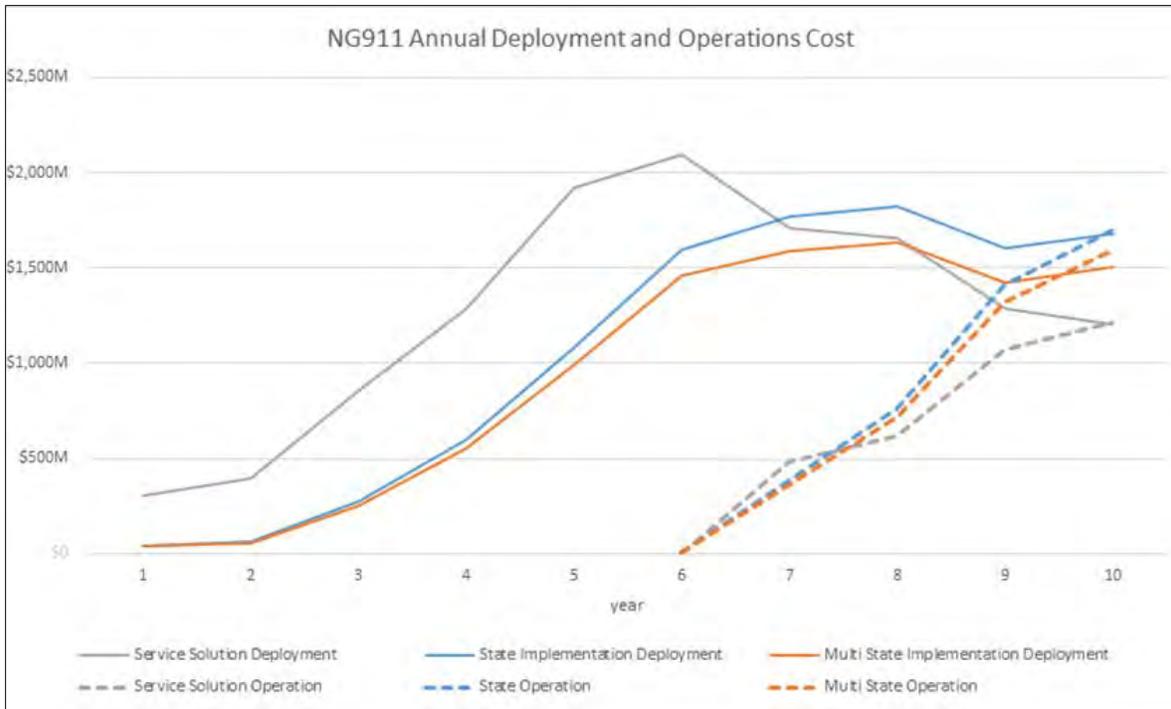
Figure 10: NG911 Annual Deployment and Operations Cost

5.1.   Implementation Scenarios

5.1.1.   State Implementation Scenario Results

The state implementation is where independent states and territories purchase, implement, and operate their own NG911 independent solution with a minimum of two NGCS centers

Figure 14 summarizes the deployment costs of NG911 by allocation for the state implementation scenario. Approximately one-third of the total ten-year cost is allocated against NGCS and another one-third to PSAPs. The remaining cost is allocated against the OSPs, and state and federal allocation groups based on the operator of each element. While these costs are allocated to these groups, this does not always result in these groups paying the costs, as many 911 costs are passed to the PSAPs today.
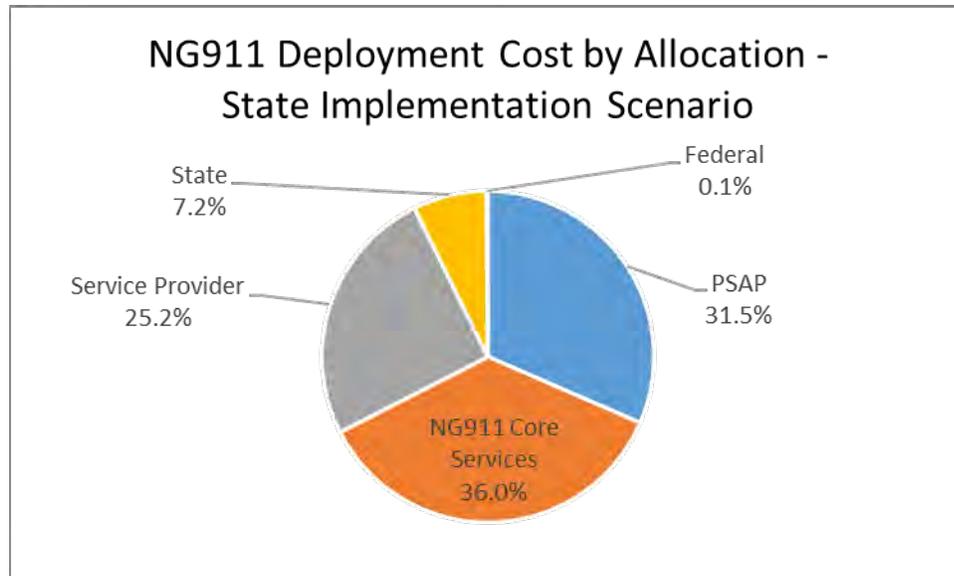
Figure 11: NG911 Deployment Cost Allocation – State Implementation Scenario

Figure 15 summarizes the breakdown of the NG911 deployment cost by NG911 Maturity Model domain for the state implementation scenario. The majority of hardware, software, and services required for implementing the NG911 end state is captured under the Applications and Systems Domain (lighter blue). As more states implement NG911 systems, the total annual costs increase.
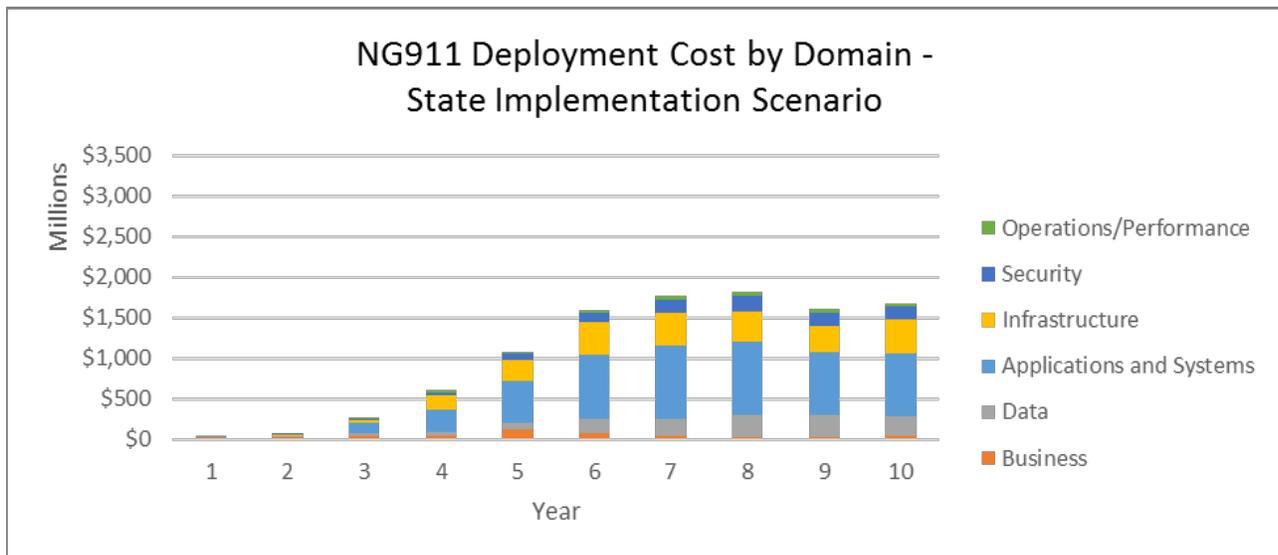
Figure 12: NG911 Deployment Cost by Domain – State Implementation Scenario

Infrastructure is the second-largest cost category (yellow), as shown in Figure 15, and accounts for all connectivity and bandwidth costs needed for the NG911 end state. Again, as more states advance in their NG911 systems deployment these costs increase, driven in part by expected increases in the multimedia functionality of all data that must be handled in real time and stored. The last year of the analysis should be generally flat with the next few years after the analysis, then decline slightly. Assuming a future optimal maintenance strategy, thereafter should remain steady (plus some accounting for inflation).

Figure 16 below demonstrates the NG911 deployment costs for the state implementation scenario broken down by FEMA regions. It is important to recognize that this cost breakdown is the result of the current status and individual unique demographic requirements—such as the number of states in the region, population, number of PSAPs, and deployment schedule—in achieving the end state. Specific characteristics of each region, in addition to an assessment of their NG911 deployment readiness, has resulted in the following deployment costs.
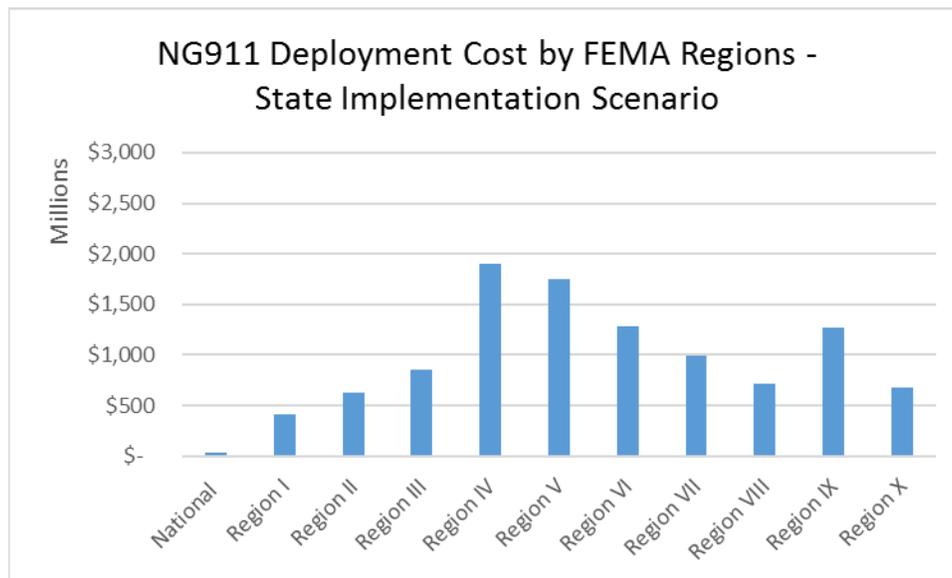
Figure 13: NG911 Deployment Cost by FEMA Region – State Implementation Scenario

5.1.2. Multistate Implementation Scenario Results

The multistate implementation is where multiple states and territories within ten geographical areas coordinate to purchase, implement, and operate shared, mega-sized NGCS centers.

Figure 17 below summarizes the deployment cost of NG911 at the nationwide-level by allocation for the multistate implementation scenario. This scenario assumes two mega-sized NG911 core service centers for each multistate area or FEMA region, compared with the individual state implementation scenario. For this reason, the NGCS operating entity allocation is less, and the

PSAP cost allocation accounts for the largest portion of this scenario. The remaining cost is allocated to OSPs, and state and federal allocation groups based on the operator of each element. While these costs are allocated to these groups, this does not always result in these groups paying the costs, as many 911 costs are passed to the PSAPs today.
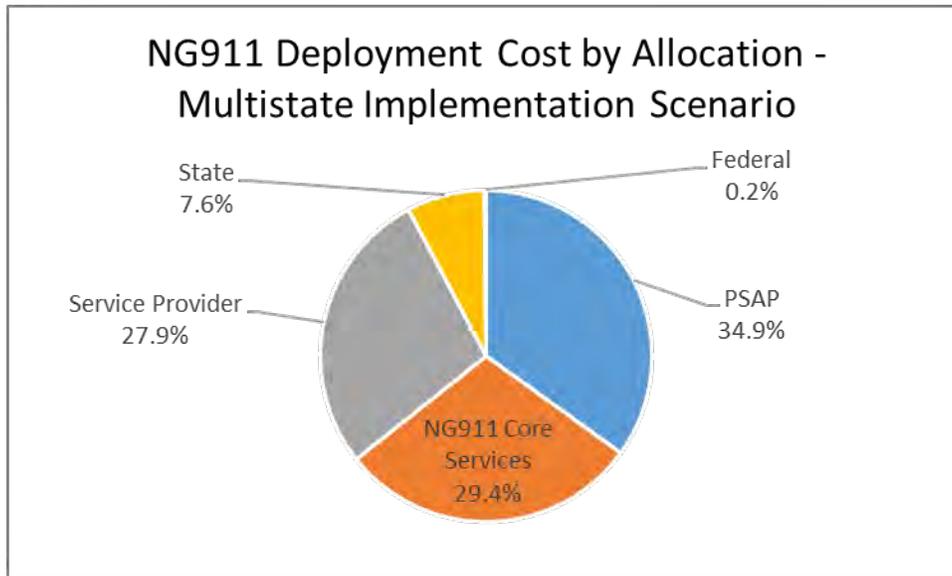
Figure 14: NG911 Deployment Cost Allocation – Multistate Implementation Scenario

Figure 18 summarizes the breakdown of the NG911 deployment costs by domain for the multistate implementation scenario. Similar to the state implementation scenario, the largest category of cost is accounted for in the Applications and Systems Domain (lighter blue), which captures most of the deployed hardware, software, and services required for achieving the NG911 end state. As more states implement NG911 systems, the total annual costs increase.
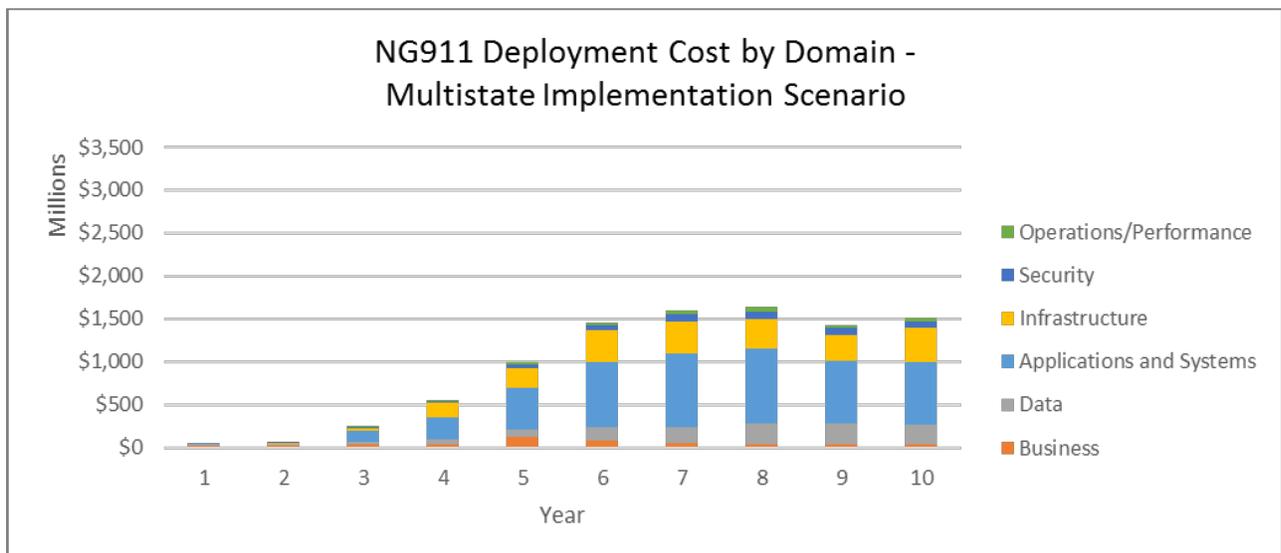
Figure 15: NG911 Deployment Cost by Domain – Multistate Implementation Scenario

Infrastructure is the second-largest cost category (yellow), as shown in Figure 18, and accounts for all connectivity and bandwidth costs needed for the NG911 end state. Again, as more states advance in their NG911 systems deployment, these costs increase.

Figure 19 below identifies the NG911 deployment costs for the multistate implementation scenario by FEMA regions. These results summarize the cost of deploying two mega NG911 core service centers within each FEMA region, in addition to small core systems at the geographically isolated U.S. territories.
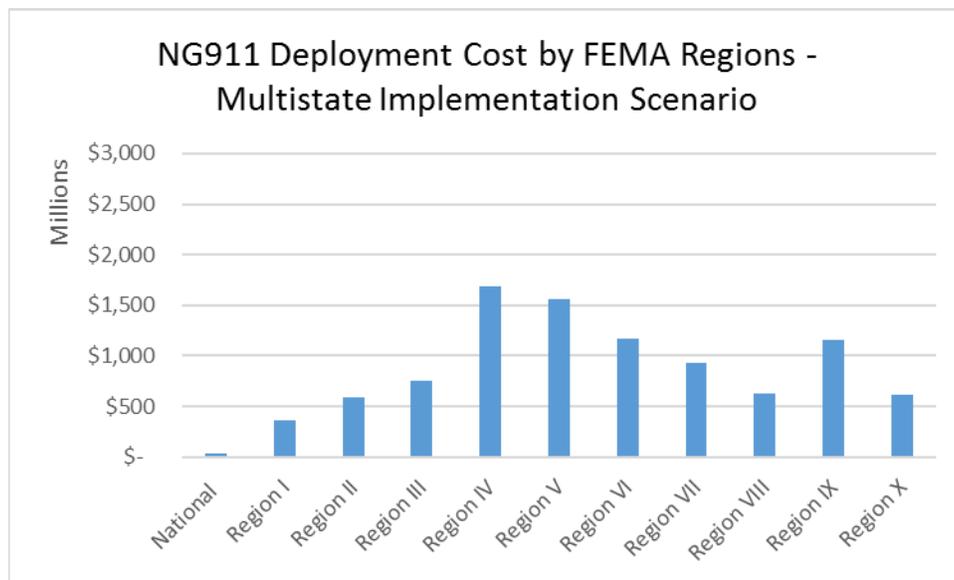
Figure 16: NG911 Deployment Cost by Region – Multistate Implementation Scenario

5.1.3. Service Solution Scenario Results

The service solution implementation is where independent states and territories purchase from an NG911 service provider all core services and PSAP system maintenance.

For the service-solution scenario, it is assumed that all core services from major service providers would instead be utilized for every state. As stated earlier, this option is architecturally similar to the multistate implementation scenario, namely there are fewer larger core service centers serving larger areas. Therefore, that scenario was utilized as a proxy for the costs that service providers incur to generate viable NG911 services. The costs for services from the multistate implementation scenario were used as the starting point for this alternative, and were cross-checked with data received from some vendors for the applicable elements of this scenario. As this is not a pricing

verification or realism analysis of any specific vendor, the only conclusion is that this estimate or cost estimate appears to correlate with the service costs that the states may pay for a service contract.

The available data, as well as the various unique requirements and implementations of individual states, is not enough to guarantee that prices currently quoted by service providers are appropriate for long-term viability of the service providers and the services they provide. While this option smooths spikes in a state's expenditure, it was not verified that these prices will stay the same for all states, and may fluctuate between them.

For purposes of the analysis, the costs are broken down into three categories:
- Annualized investment and refresh service costs represent the initial acquisition and maintenance costs of PSAPs and NGCS through a hosted solution.
- Annualized operations service costs represent the ongoing operations and maintenance costs of PSAPs, ESInets, and NGCS.
- Annualized non-service costs represent all additional costs allocated to service providers, state, and federal entities, similar to those contained within the multistate implementation scenario.

Figure 20 summarizes the deployment cost of NG911 for the service-solution scenario. The annualized service costs presented are susceptible to market forces of any individual vendor's approach for bidding to be a state provider. An analysis would be expected for a state to decide if the benefits to them outweigh what was proposed, as they could possibly even save money over ten years depending on market conditions in their circumstance.
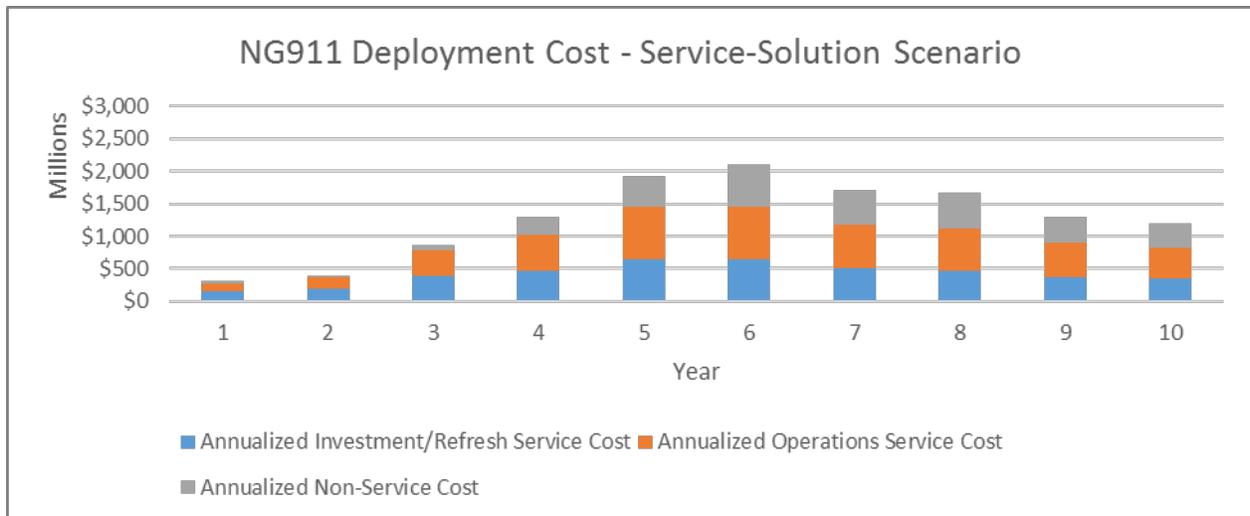
Figure 17: NG911 Deployment Cost – Service-Solution Scenario

In the deployment of NG911, the overall premium paid out in the service-solution scenario is almost $2.2 billion greater than the individual state implementation. Under the service-solution scenario, the vendor is expected to maintain and upgrade all equipment for the annual service price. This essentially includes the refresh costs back inside the deployment window, resulting in the larger value.

5.2.   Future Impacts to the Results

There are two major future impacts to the actual costs of NG911 implementation. These impacts are the deployment method and the time frame of the deployment.

While each scenario assumes that the entire country will utilize a homogeneous path forward, it is expected that with federal and state budget and planning realities, this is highly unlikely. Therefore, the cost of the nationwide solution will be a combination of all alternatives. The states that have begun to deploy NG911 services are leaning toward the service-solution model, but there is no clear trend due to the limited numbers of deployments to date.

The second impact is the deployment time frame. This study used a combination of four and six years. These are technically feasible, but the planning and governance requirements in some cases may delay this further.

The cost model was used for a comparison of the time frame of the costs based on the four- and six-year models. All current progress and variables were removed and just the time frame variable remained. The analysis found that the six-year deployment added approximately 35 percent more cost to the deployment compared with the four-year deployment. While an analysis of the cause of this increase was not performed, the time that systems were in place during a six-year deployment was longer, so some recurring costs likely would be incurred for a longer period.

It is important to note that this does not examine the ability of some states to coordinate the complex migration within those time frames. It is expected that the time frames will become shorter as migrations become more common. Some states that are in the process of migrating to NG911 today have been working for more than six years to deploy transitional elements.

This page is intentionally left blank.

6.   CONCLUSIONS

6.1.   Background

The National 911 Program conducted an NG911 Cost Study that "analyzed and determines detailed costs" for a nationwide implementation of NG911, as required by Congress in the Middle Class Tax Relief and Job Creation Act of 2012 (P.L. 112-96).

By statute, "the purpose of the report is to serve as a resource for Congress as it considers creating a coordinated, long-term funding mechanism for the deployment and operation, accessibility, application development, equipment procurement, and training of personnel for Next Generation 911 services." The report also must include the following:

- Information on how costs would be broken out geographically and allocated among PSAPs, broadband service providers, and third-party providers of NG911 services
- An assessment of the current state NG911 service readiness among PSAPs
- Information on how differences in PSAP access to broadband across the United States might affect costs
- A technical analysis and cost study of different delivery platforms, such as wireline, wireless, and satellite
- An assessment of architectural characteristics, feasibility, and limitations of NG911 service delivery
- An analysis of the needs for NG911 services of persons with disabilities
- Standards and protocols for NG911 services, and for incorporating VoIP and "Real-Time Text" standards

6.2.   NG911 Architecture

NG911 is an enterprise solution that will result in a nationwide system of systems that must share a common approach and be interoperable. To complete the cost study, a framework was needed that would provide:

- A breakdown of elements to a level that can be assigned a cost
- A breakdown of elements to a level that can be measured
- A breakdown of elements that can be used to measure progress

The NG911 Maturity Model was developed to accomplish these goals and was used throughout the NG911 Cost Study Project.

The NG911 Maturity Model uses the following components:

- NG911 Maturity Stages – Time frames of the NG911 transition
  - Legacy
  - Foundational
  - Transitional
  - Intermediate
  - End State
- NG911 Framework – Various functions and systems that are transitional steps or required for NG911
  - Domains – Major areas of focus
    - Business
    - Data
    - Applications and Systems
    - Infrastructure
    - Security
    - Operations/Performance
  - Functional components – Specific functional or operational components of NG911 that are performed within the domain
  - Elements – Specific actions implemented or systems deployed

Next Generation 911 Maturity Model

Figure 18: NG911 Maturity Model

The NG911 Maturity Model was focused on the functions that are performed in an NG911 environment. In addition, a traditional architecture drawing was developed that identified the physical systems and devices that will be used. (Appendix A, Section A.2 – Architecture contains an enlarged version of the diagram.)
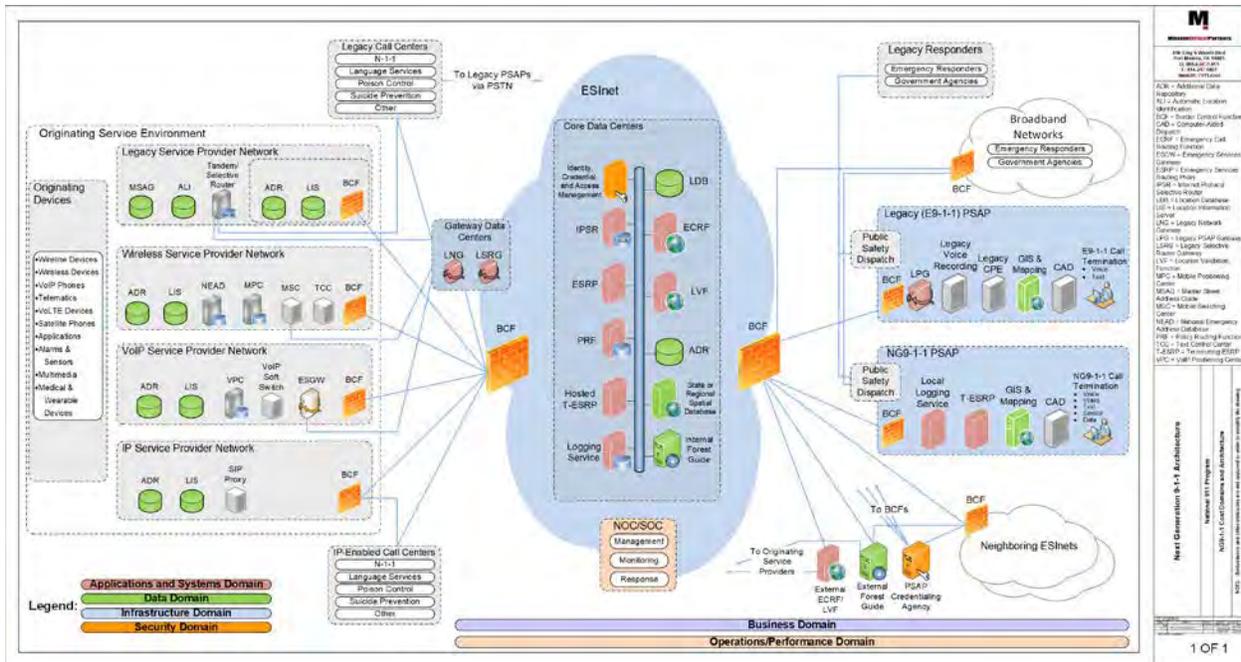
Figure 19: NG911 Architecture

6.3.   Current Environment

In many cases, states are implementing NG911 networks incrementally, as circumstances enable their ability to plan for, fund, and carry out deployment. The purpose of the National Profile Database data collection was to identify states that are at least advancing NG911 capabilities and components. It should be noted that data self-reported by 911 authorities without a single universally accepted definition of NG911 may not permit confident conclusions.

A review of the current status of NG911 implementation used in this study readily illustrates the various stages of readiness. Over the past three years, progress has been exceedingly slow.

The NG911 current status shows that the Business Domain is well into the early majority, as defined by the Innovation Adoption Lifecycle, with 26.4 percent of the nation beyond the legacy stage. The next largest domain is Applications and Systems, which is also into the early majority, with 20.8 percent of the nation beyond the legacy stage. Additional implementations in the Infrastructure, Data, and Security Domains are in the early adopters, but have begun. The laggard seems to be the Operations/Performance Domain, which is understandable as many of the systems are still in the implementation or early service life phases.

Table 8: NG911 Current Status

	Legacy	Foundational	Transitional	Intermediate	End State
Business Domain	73.6%	16.4%	2.9%	7.1%	
Data Domain	89.0%		8.2%	2.8%	
Applications and Systems Domain	79.2%	10.0%	1.0%	9.8%	
Infrastructure Domain	88.2%	10.2%		1.6%	
Security Domain	86.9%	7.1%	6.0%		
Operations/ Performance Domain	98.0%	2.0%			

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

Just as the definition of NG911 is varied, the way 911 service has been implemented throughout the country is equally varied because such service traditionally has been jurisdictionally siloed. This diversity of implementations and local preference has given rise to a strong desire to continue to do things in a local way. In some cases, state statute assigns decision-making for 911 operations to the lowest level of local government, to ensure that the response requirements are kept local.

6.4.   Cost Analysis Framework

The NG911 Maturity Model was used as the framework for the cost study. Each element of the NG911 Maturity Model was identified in terms of cost, scaling, timing, and category, which are all included within the cost model. Three NG911 implementation scenarios were analyzed with the cost model: state implementation, multistate implementation, and a service-solution scenario. Table 11 below describes each scenario.

Table 9: NG911 Implementation Scenarios

Scenarios	Description
State Implementation	Fully independent states and territories with a minimum of two NGCS centers
Multistate Implementation	Multiple states within ten geographical areas coordinate and leverage from shared, mega-sized NGCS centers
Service Solution	Fully independent states utilize an NG911 service provider for all core services and PSAP system maintenance

Cost estimation for each geographical region, consisting of multiple states, was conducted with specific SME inputs, including locality factors and progress status (i.e., the NG911 current status) for each element. Results of the elements were then extrapolated to the entire nation using appropriate scaling factors to provide a ten-year total NG911 implementation cost estimate. Some high-level ground rules and assumptions utilized in this analysis are as follows:

- Costs of operating and maintaining the current legacy 911 systems are not included within this analysis
- Achieving the desired NG911 end state is scheduled for all states and territories within ten years of initiation
- The costs associated with federally operated PSAPs were not included in this study
- For optimal organization at the nationwide level, each state should have a single authoritative entity for its NG911 network
- States will be responsible for implementing and maintaining their own infrastructure; therefore, consolidations and shared infrastructure, while important, are out of scope
- The current number of PSAPs[28] is sufficient to serve the population of each respective region/municipality
- Cost data sources include publicly available data from NG911 estimates, vendor information, government contracts and other publicly available cost information at a state or multistate level

6.5.   Cost Analysis

Table 12 below shows the total cost that is required for just the deployment of nationwide-level NG911 systems within each scenario. These deployment cost estimates incorporate only the costs required for the initial setup and migration to full NG911 systems for each state/region. The deployments are spread over the ten-year lifecycle using a combination of four- to six-year initial deployments, and include a two-year transition from the legacy systems. Therefore, some ongoing operations and maintenance costs of states that may reach the NG911 end state before year 10 are excluded from these totals.

As compared with the full ten-year cost, the deployment costs within all scenarios are decreased due to not including refresh costs and ongoing operational costs beyond the deployment; however, the overall premium paid out in the service-solution scenario is almost $2.2 billion greater than the individual state implementation. This can be explained for the primary implementation scenarios by removing the equipment refresh outside of this deployment window, while under the service-

---

[28] Derived from combining the latest available *2016 National 911 Progress Report*, FCC's *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, and the FCC's Master PSAP Registry.

solution scenario, the vendor would be expected to maintain and upgrade all of the equipment within the established annual service price.

Table 10: NG911 Total Deployment Cost Estimation

Cost Type	State Implementation	Multistate Implementation	Service Solution
One-Time Costs	$3,022.3M	$2,898.8M	$599.3M
Recurring Costs	$7,508.1M	$6,606.5M	$12,115.3M
Total	**$10,530.4M**	**$9,505.3M**	**$12,714.6M**

Figure 23 below depicts the year-by-year deployment excursions for the three implementation scenarios. For the state and multistate implementation scenarios, costs begin to decrease in years 8 and 9 as early-adopting regions and fast implementers have surpassed their end state by two years; the cost increases in year 10 represent the slow-adopting regions just reaching their first full year of operation. Meanwhile the service-solution scenario shows a faster increase as the multistate areas begin implementation, which includes maintaining the entire planned service in perpetuity, and a decrease as the end state is achieved.
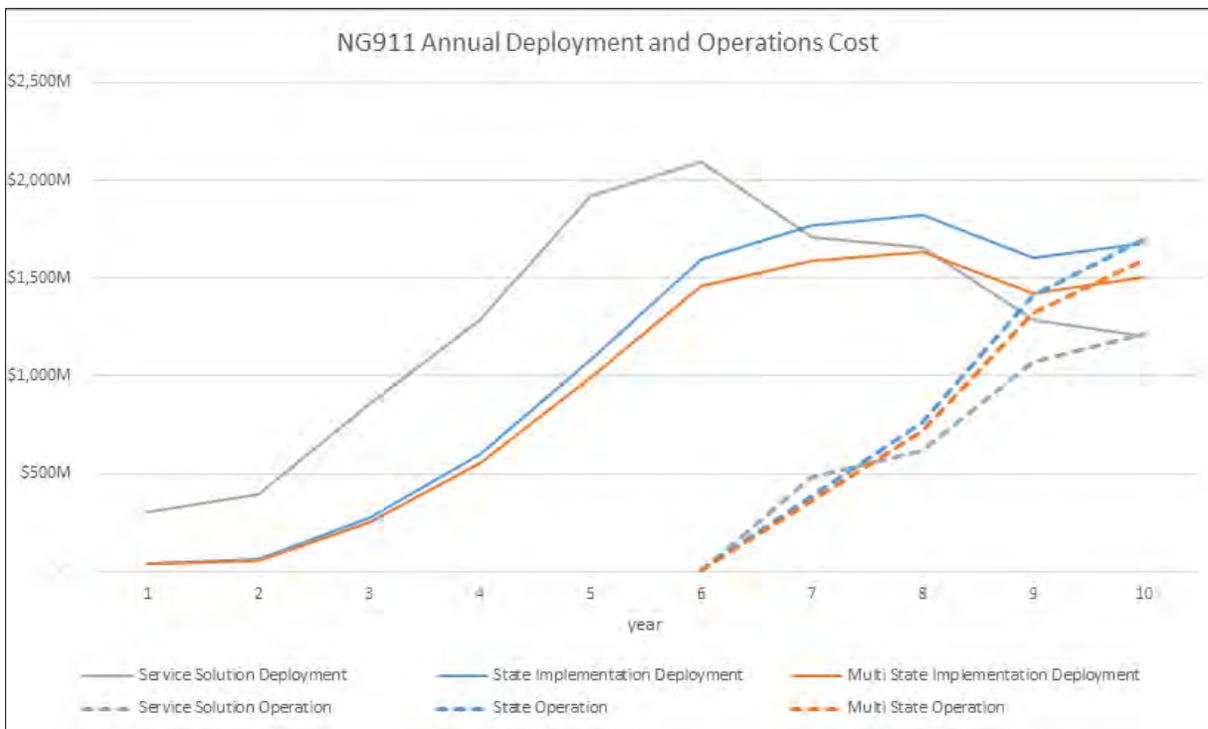
Figure 20: NG911 Annual Deployment and Operations Cost

6.6.   Section 6508 Summary

1. *How costs would be broken out geographically and allocated among public safety answering points, broadband service providers, and third-party providers of Next Generation 9-1-1 services.*

To arrive at an answer regarding how to break out the costs geographically, the cost study used the ten FEMA regions. Figure 24 below identifies the total NG911 deployment costs, by FEMA regions, for the state implementation scenario. It is important to recognize that this cost breakdown is based upon the NG911 Maturity Model current status and individual unique demographic requirements for each FEMA region in achieving the end state. Factors such as the number of states per region, population, number of PSAPs, and deployment schedule, impact the NG911 deployment costs per geographic region.
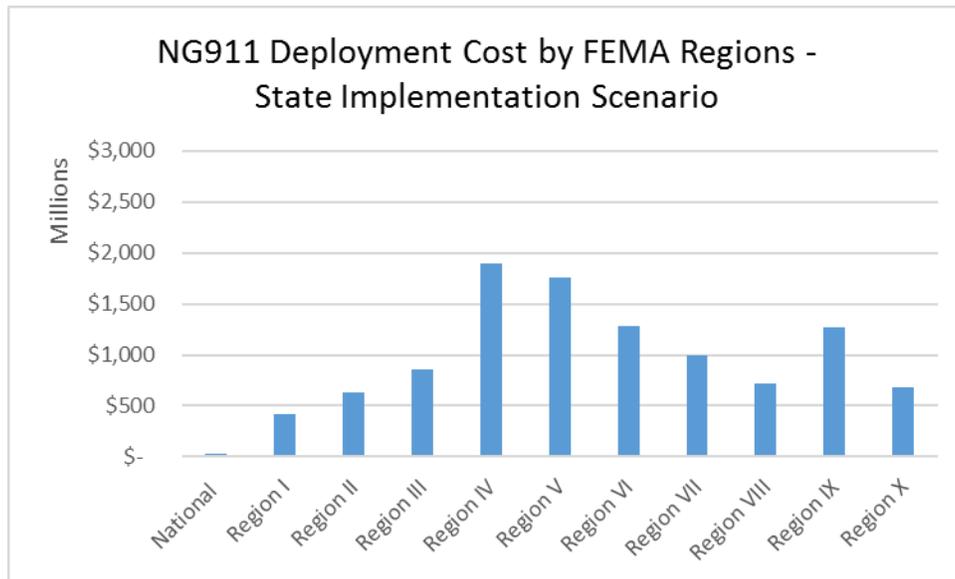
Figure 21: NG911 Deployment Cost by FEMA Regions – State Implementation Scenario

Still using the costs for the state implementation scenario, Figure 25 summarizes the NG911 deployment costs by allocation. Each element was associated with an operating entity allocation tag so that the costs could be allocated appropriately within the NG911 system of systems. The cost study identified the following operating entities for cost allocation: PSAPs, state authorities, NGCS providers, and service providers. However, this allocation may not relate directly to the entity that would pay those costs because allowable 911 costs vary across the nation, as each state allocates the costs differently. Approximately one-third of the total deployment cost is allocated against NGCS and another one-third to PSAPs. The remaining cost is allocated against the OSPs, and state and federal allocation groups.
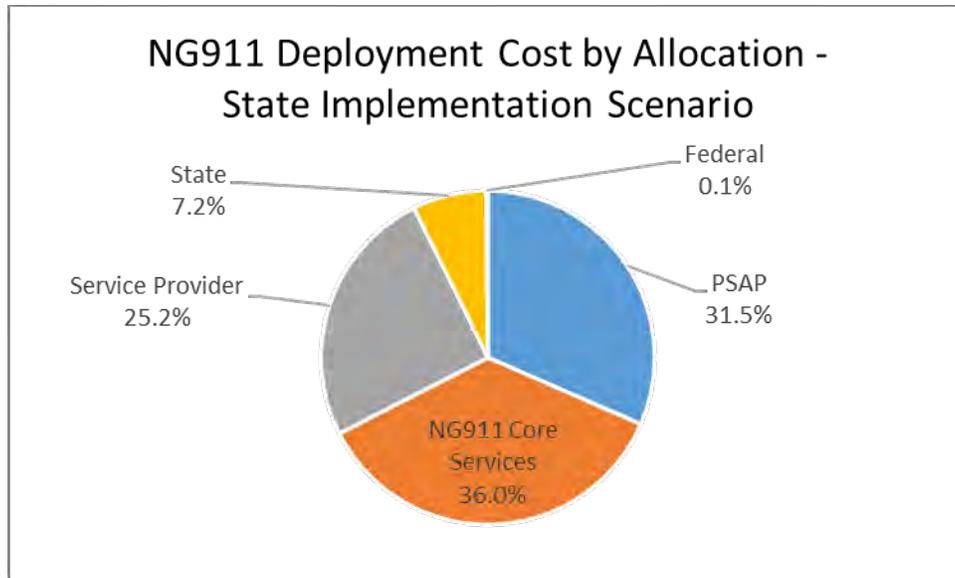
Figure 22: NG911 Deployment Cost Allocation - State Implementation Scenario

Detailed information and costs are located in Sections 4 and 5, as well as Appendix E.

2. *An assessment of the current state of Next Generation 9-1-1 service readiness among public safety answering points.*

NG911 readiness is larger than just the PSAP. While a PSAP may have fully complete systems and be defined as being NG911 ready, there are other factors—such as the NGCS, connectivity, and data outside of the PSAP—that will impact the readiness. The NG911 Maturity Model is used to measure progress toward NG911 as a whole. The model contemplates the PSAP readiness for multiple elements in multiple domains for each state, and compiles the data into a percentage complete for each stage of the NG911 Maturity Model. For example, using the available self-reported information from the National Profile Database and the FCC, about 55 percent of the nation's population is covered by a PSAP with IP-capable call-handling equipment. As a result, 55 percent of the nation's population can be considered to have call-handling equipment meeting requirements for the Intermediate stage. The data for other PSAP systems required to fully utilize NG911 information and functions, such as logging recorders and computer-aided dispatch (CAD), is not well-tracked, and with the lack of available data these systems are assumed to be in the legacy stage.

Detailed information on NG911 readiness is included in Section 3 and Appendix B.

3. *How differences in public safety answering points' access to broadband across the United States may affect costs.*

The cost study applied geographic factors within the cost model to account for changes in costs as defined within current federal government contracts for broadband service. However, while some rural areas have more distance and often higher costs, they additionally have lower broadband needs, in some cases balancing out. However, concerning the Pacific Islands, broadband was identified as a particularly high cost area. Due to the nature of the cost study, for most CONUS[29] locations, these costs were averaged across the entire country. With the widespread availability of various broadband methods across the country, and with the PSAP sizes determining the minimum requirements, these averages seem appropriate.

Additional detail is included in appendices C, D, and E.

4. *A technical analysis and cost study of different delivery platforms, such as wireline, wireless, and satellite.*

Many of the major telephone providers publicly have announced their plans to migrate from their legacy technologies to IP-based systems, with progress currently underway. The speed at which the originating service providers (OSPs) migration will impact the time frame the Legacy gateways will need to remain in place. Appendix A describes the standards of the NG911 Maturity Model. The OSPs have little impact in the NG911 end state, but will require coordination during the migration. Each OSP will deliver calls to the NG911 system in an industry-standard format. The NG911 ingress network design is standards-based, and thus should remain delivery-platform agnostic. Therefore, appropriately establishing NG911 results in the same costs for NG911, regardless of the delivery platform. Due to these factors, there is no major technical impact expected on NG911 deployment, but if the time frame is extended, then some transitional elements may need to operate longer, which will result in increased total cost.

Additional detail can be found in Section 2.4, as well as appendices A and C.

5. *An assessment of the architectural characteristics, feasibility, and limitations of Next Generation 9-1-1 service delivery.*

Appendix C describes these in detail. NG911 has been shown to be feasible by regions and states that have deployed components at a variety of stages of the NG911 Maturity Model. These early-adopter deployments have proven the viability of individual components and identified areas

---

[29] Contiguous United States

within the standards that need further refinement and/or development. The greatest limiting factors to NG911 deployment are the challenge of coordinating the various entities, the provisioning of legacy transitional elements to provide backward compatibility, and funding. Leap-frogging the limitations or shortening the time needed for backward compatibility would significantly speed the time to deployment and reduce the overall cost of implementation.

Additional detail can be found in Section 2.4, as well as appendices A and C.

6. *An analysis of the needs for Next Generation 9-1-1 services of persons with disabilities.*

Barriers to 911 access for functional needs populations such as the Deaf and Hard of Hearing community are becoming more widely understood and their concerns more readily embraced. Equal-access requirements state that, today, PSAPs must accept a call from a person with a hearing or speech disability. While an interim SMS text solution is available prior to full implementation of NG911, the feature-rich benefits of text-to-911, real-time text, multimedia, or other wireless device applications only can be realized with NG911 End State implementation.

Additional considerations for NG911 services for persons with disabilities concern the potential to receive additional information that supports the PSAP's knowledge of the individual calling 911. The Additional Data Repository (ADR) may contain additional subscriber information, such as medical information and emergency contact information. This additional information can be recognized with implementation of NG911, and can help support persons with disabilities by providing additional detail to support them when they place an emergency call.

Additional detail regarding the impact of NG911 on the functional needs community can be found in Section 2.4, as well as Appendix C – Section C.3.

7. *Standards and protocols for Next Generation 9-1-1 services and for incorporating Voice over Internet Protocol and "Real-Time Text" standards.*

There are many standards and protocols that are required for NG911 implementation. Those currently available, as well as those that are in development, are identified in Appendix A. Areas that require further development or new standards may be found in Appendix A and Appendix C.

This page is intentionally left blank.

ACRONYMS LIST

Acronym	Definition
#	Pound
*	Star
3GPP	3rd Generation Partnership Project
AACN	Advanced Automated Collision Notification
ADA	Americans with Disabilities Act
ADR	Additional Data Repository
ALI	Automatic Location Identification
ANI	Automatic Number Identification
APCO	Association of Public-Safety Communications Officials International
ATIS	Alliance for Telecommunications Industry Solutions
BCF	Border Control Function
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol 4
CAD	Computer Aided Dispatch
CALC	Contract Awarded Labor Category
CAMA	Centralized Automatic Message Accounting
CER	Cost Element Relation
CERT	Computer Emergency Readiness Team
CERT	Cyber Emergency Response Team
CES	Cost Element Structure
CFR	Code of Federal Regulations
CJIS	Criminal Justice Information Services
CLDXF	Civic Location Data Exchange Format
ConOps	Concept of Operations
CONUS	Contiguous United States
COOP	Continuity of Operations Plan
CPE	Customer Premises Equipment
CSP	Competitive Service Provider
CTO	Communications Training Officer
DHS	Department of Homeland Security
DOJ	Department of Justice
DOT	United States Department of Transportation
DS Field	Differentiated Services Field
DSCP	Differentiated Services Code Point
E2	Emergency Service Protocol

Acronym	Definition
EAAC	Emergency Access Advisory Committee
EC3	Emergency Communications Cybersecurity Centers
ECRF	Emergency Call Routing Function
EDXL-DE	Emergency Data Exchange Language Distribution Element
EIDD	Emergency Incident Data Document
ESInet	Emergency Services Internet Protocol Network
ESMI	Emergency Services Messaging Interface
ESN	Emergency Service Number
ESRP	Emergency Services Routing Proxy
EV-DO	Evolution-Data Only
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEAF	Federal Enterprise Architecture Framework
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FirstNet	First Responder Network Authority
FTE	Full-time Equivalent
GAO	Government Accountability Office
GEOPRIV	Geographic Location/Privacy
GIS	Geographic Information System
GR&As	Ground Rules and Assumptions
GS	General Schedule
GSA	General Services Administration
HELD	HTTP-Enabled Location Delivery
HSPA	High-Speed Packet Access
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW/SW O&M	Hardware/Software Operation and Maintenance
I2F	ISE Information Interoperability Framework
ICAM	Identity, Credential, and Access Management
ICO	Implementation Coordination Office
IDP	Intrusion Detection and Prevention
IDPS	Intrusion Detection and Prevention Services
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILEC	Incumbent Local Exchange Carrier
IMS	IP Multimedia Subsystem

Acronym	Definition
IoT	Internet of Things
IP	Internet Protocol
IP CTS	Internet Protocol Captioned Telephone Service
IPS	Intrusion Prevention System
IPSR	IP Selective Router
IS	Identity Searchable
ISE	Information Sharing Environment
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
kbps	Kilobits per Second
LCCE	Lifecycle Cost Estimation
LCD	Liquid Crystal Displays
LDB	Location Database
LEC	Local Exchange Carrier
LIF	Location Interwork Function
LIS	Location Information Server
LMR	Land Mobile Radio
LNG	Legacy Network Gateway
LOE	Labor of Effort
LoST	Location-to-Service Translation
LPG	Legacy PSAP Gateway
LSRG	Legacy Selective Router Gateway
LTE	Long-term Evolution
LVF	Location Validation Function
Mbps	Megabits per Second
MCLS	Media Communication Line Services
MCS	Master Street Address Guide Conversion Service
MF	Multi-frequency
MIB	Management Information Base
MIS	Management Information Systems
MOS	Mean Opinion Score
MPC	Mobile Positioning Center
MSAG	Master Street Address Guide
MSC	Mobile Switching Center
MSRP	Message Session Relay Protocol
NEAD	National Emergency Address Database

Acronym	Definition
NENA	National Emergency Number Association
NFPA	National Fire Protection Association
NG	Next Generation
NG911 or NG9-1-1	Next Generation 911
NGCS	Next Generation Core Services
NGIIF	Next Generation Interconnection Interoperability Forum
NGN	Next Generation Network
NG-SEC	NENA Security for Next-Generation 9-1-1 Standard
NHTSA	National Highway Traffic Safety Administration
NID	NENA Emergency Services IP Network Design for NG9 1-1
NIDCD	National Institute on Deafness and Other Communication Disorders
NIEM	National Information Exchange Model
NIF	Interwork Function
NIST	National Institute of Standards and Technology
NNI	Network-to-Network Interface
NOC	Network Operations Center
NORS	Network Operations Reporting System
NPSBN	Nationwide Public Safety Broadband Network
NS/EP	National Security and Emergency Preparedness
O&M	Operation and Maintenance
OMB	Office of Management and Budget
OMG	Object Management Group
OPM	Office of Personnel Management
OSE	Originating Service Environment
OSP	Originating Service Provider
OSPF	Open Shortest Path First
PBX	Private Branch Exchange
PC	Personal Computer
PIDF	Presence Information Data Format
PIDF-LO	Presence Information Data Format Location Object
PIF	Protocol Interworking Function
PRF	Policy Routing Function
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QC	Quality Control
QoS	Quality-of-Service
RFAI	Request for Assistance Interface

Acronym	Definition
RFC	Request for Comments
RFP	Requests for Proposal
RMS	Records Management Systems
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SCC	Standards Coordinating Council
SCIP	Statewide Communications Interoperability Plan
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIPREC	SIP-based Media Recording
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol, version 3
SOC	Security Operations Center
SOI	Service Order Input
SOP	Standard Operating Procedure
SOW	Scope of Work
SR	Selective Router
SS7	Signaling System 7
TCC	Text Control Center
TDD	Telecommunications Device for the Deaf
TDM	Time Division Multiplexing
T-ESRPs	Terminating ESRPs
TFOPA	Task Force on Optimal Public Safety Answering Point Architecture
the Act	Middle Class Tax Relief and Job Creation Act of 2012
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TRS	Telecommunications Relay Services
TTFF	Time to First Fix
TTY	Teletypewriter
U.S.	United States
UC	Unified Communications
UML®	Unified Modeling Language™
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USM	User-based Security Model

Acronym	Definition
VACM	View-based Access Control Model
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Center
VRS	Video Relay Service
VSP	VoIP Service Provider
WG2	Working Group 2
XML	Extensible Markup Language

APPENDIX A – NG911 ARCHITECTURE

A.1. NG911 Framework Domains

A.1.1. BUSINESS DOMAIN

The Business Domain consists of those planning and procurement activities that must take place to lay the groundwork for a transition to Next Generation 911 (NG911). These activities are illustrated in the matrix found in Figure A-1 below.

Next Generation 911 Business Domain

	LEGACY	FOUNDATIONAL	TRANSITIONAL	INTERMEDIATE	END STATE
PLANNING		Establish NG911 Plan	Concept of Operations		Annually Reviewed
GOVERNANCE	Gap Analysis		Governance Plan		Annually Reviewed
POLICY	Gap Analysis		Established and Annually Reviewed Policies		
NATIONAL GOVERNANCE	Gap Analysis		Governance Plan		Annually Reviewed
PROCUREMENT		Procurement Activities throughout Process			
IMPLEMENTATION		Statewide Coordination / Implementation Project Management			

Figure A-1: NG911 Business Domain Matrix

A.1.1.1.   Planning

In the majority of states, 911 systems to date have been operated and managed on a local level, often in siloes and with an independent approach. NG911 is an entirely different concept than what currently exists. More integration and interoperability is needed to improve the effectiveness of NG911 systems. Indeed, statewide coordination is essential for effective NG911 implementation, and operating a statewide 911 system is more complicated than operating a local 911 system. Statewide 911 planning may or may not exist at the Legacy stage. There are two elements of planning, described below.

- Statewide NG911 Plan – A statewide plan should be created explaining how NG911 will be deployed within the state.[30] The statewide plan is developed in the Foundational stage. In those states without a statewide 911 authority, it is possible that an NG911 plan may be created at a regional level.

Functional & Technical Requirements	Specifications/Standards
Identify stakeholders and establish roles and responsibilities	- Report for National 9-1-1 Assessment Guidelines - NENA Next Generation 9-1-1 Transition Policy Implementation Handbook - NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document - SAFECOM Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials

---

[30] "Draft Report for National 9-1-1 Assessment Guidelines," 911 Resource Center, June 2012, https://resourcecenter.911.gov/911Guidelines/RPT053012_National_911_Assessment_Guidelines_Report_FINAL.pdf, section 5.2.

Functional & Technical Requirements	Specifications/Standards
Describe technical architecture of solution	• Report for National 9-1-1 Assessment Guidelines • NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook • Task Force on Optimal Public Safety Answering Point Architecture (TFOPA), Working Group 2 (WG2), Final Report, December 10, 2015
Identify funding sources	• Report for National 9-1-1 Assessment Guidelines • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook
Provide high-level timeline for the plan	• Report for National 9-1-1 Assessment Guidelines

- <u>NG911 Concept of Operations</u> – A detailed concept of operations (ConOps) should be created to guide the transitional process. The ConOps is developed in the Transitional stage and is used through the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
Governance, communications plan, budget and funding	• NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document • Report for National 9-1-1 Assessment Guidelines • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook

Functional & Technical Requirements	Specifications/Standards
Detailed technical specifications and diagram	• NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document • NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document
Timeline of transition	• NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook
Deployment and testing of plan	• NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document
Roles and responsibilities of all stakeholders	• NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook

- <u>Annually Review and Update Statewide NG911 Plan</u> – A statewide plan should be annually reviewed and updated to reflect the current environment.

Functional & Technical Requirements	Specifications/Standards
Identify stakeholders and establish roles and responsibilities	• Report for National 9-1-1 Assessment Guidelines • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook • NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document

Functional & Technical Requirements	Specifications/Standards
Identify stakeholders and establish roles and responsibilities (continued)	• SAFECOM Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials
Describe technical architecture of solution	• Report for National 9-1-1 Assessment Guidelines • NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook • TFOPA, WG2, Final Report, December 10, 2015
Identify funding sources	• Report for National 9-1-1 Assessment Guidelines • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook
Provide high-level timeline for the plan	• Report for National 9-1-1 Assessment Guidelines

A.1.1.2.   Governance

In the majority of states, legacy 911 service currently is operated on a local level. To implement NG911 on a regional, tribal, state, or nationwide basis, a governance model needs to be established. Key elements of such an initiative include a gap analysis and a plan.

- Governance Gap Analysis – Even those states that have a statewide 911 authority will need to perform a governance gap analysis. It may be necessary to update state statutes prior to moving forward with NG911 planning and transition. The gap analysis is started during the Legacy stage.

Functional & Technical Requirements	Specifications/Standards
Statute review process	• Report for National 9-1-1 Assessment Guidelines • NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document
Sustainable funding	• Report for National 9-1-1 Assessment Guidelines
Authorization to coordinate statewide NG911 system	• Report for National 9-1-1 Assessment Guidelines
Inter-local cooperation is allowed	• Report for National 9-1-1 Assessment Guidelines
Authority to procure statewide NG911 components	• Report for National 9-1-1 Assessment Guidelines

- Governance Plan – The state should collaborate with stakeholders to create a comprehensive governance plan for the NG911 system. Even in those areas that have implemented a regional plan and NG911 system, statewide governance is needed to ensure interoperability between regions. The governance plan is developed and implemented in the Foundational through Intermediate stages.

Functional & Technical Requirements	Specifications/Standards
Identify stakeholder groups	• Report for National 9-1-1 Assessment Guidelines
Define roles and responsibilities	• Report for National 9-1-1 Assessment Guidelines • NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document
Establish authority levels	• Report for National 9-1-1 Assessment Guidelines
Determine NG911 system oversight responsibilities	• Report for National 9-1-1 Assessment Guidelines

Functional & Technical Requirements	Specifications/Standards
Prepare interjurisdictional agreement models	• Report for National 9-1-1 Assessment Guidelines • TFOPA, WG2, Final Report, December 10, 2015 • NENA-INF-012.2-2015 – Inter-Agency Agreements Model Recommendations Information Document

- <u>Annually Review Governance Plan</u> – The governance plan is reviewed and updated on an annual basis to reflect the current environment.

Functional & Technical Requirements	Specifications/Standards
Identify stakeholder groups	• Report for National 9-1-1 Assessment Guidelines
Define roles and responsibilities	• Report for National 9-1-1 Assessment Guidelines • NENA-INF-006.1-2014 – NG9-1-1 Planning Guidelines Information Document
Establish authority levels	• Report for National 9-1-1 Assessment Guidelines
Determine NG911 system oversight responsibilities	• Report for National 9-1-1 Assessment Guidelines
Prepare interjurisdictional agreement models	• Report for National 9-1-1 Assessment Guidelines • TFOPA, WG2, Final Report, December 10, 2015 • NENA-INF-012.2-2015 – Inter-Agency Agreements Model Recommendations Information Document

A.1.1.3. Policy

Policies such as security, interconnection, operation, and Identity, Credential, and Access Management (ICAM) at both the public safety answering point (PSAP) and state levels will need to be updated for the transition to NG911. Key elements of such an initiative include a gap analysis and establishment of policies.

- Policy Gap Analysis – A gap analysis should be performed to identify those policies that will need to be updated, as well as new policies that may need to be developed. The gap analysis is started in the Legacy stage and continues into the Foundational stage.

Functional & Technical Requirements	Specifications/Standards
Define standard of NG911 service	• Report for National 9-1-1 Assessment Guidelines • Association of Public-Safety Communications Officials International (APCO)/NENA ANS 1.102.2-2010 – Public Safety Answering Point (PSAP) Service Capability Criteria Rating Scale • NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)
Identify current state	• Current statutes and policies
Identify gaps and/or needs	• Report for National 9-1-1 Assessment Guidelines

- Policies – Stakeholders should create and update policies governing NG911. The state may want to provide policy templates for use by PSAPs in updating local policies specifically related to interjurisdictional operations. Policies are created in the Foundational stage and maintained into the End State, where the policies are reviewed and updated on a regular basis.

Functional & Technical Requirements	Specifications/Standards
Define training requirements	• Report for National 9-1-1 Assessment Guidelines
Determine how information/data will be shared and maintained	• Report for National 9-1-1 Assessment Guidelines

Functional & Technical Requirements	Specifications/Standards
Define requirements for network connectivity	• Report for National 9-1-1 Assessment Guidelines
Establish call routing and 911 backup plan	• Report for National 9-1-1 Assessment Guidelines
Create fund-distribution policies	• Report for National 9-1-1 Assessment Guidelines

A.1.1.4.   *National Governance*

To facilitate a nationwide transition to NG911, it will be necessary to have some level of national governance. There will be a need for states to interconnect their networks to transfer calls, synchronize geographic information system (GIS) files, and share data. National governance does not mean a federal agency must operate 911, but there needs to be coordination at a national level. Key elements of this initiative include a gap analysis and a plan.

- National Governance Gap Analysis – The gap analysis should identify the areas that require national-level governance to assist in the nationwide transition to NG911. It may be necessary to update statutes prior to moving forward with NG911 planning and transition. The gap analysis is started in the Legacy stage.

Functional & Technical Requirements	Specifications/Standards
Conduct national legislative review	• Report for National 9-1-1 Assessment Guidelines
Determine sustainable funding mechanism	• Report for National 9-1-1 Assessment Guidelines
Evaluate authority to procure national-level components	• Report for National 9-1-1 Assessment Guidelines
Explore potential intergovernmental cooperation	• Report for National 9-1-1 Assessment Guidelines

- National Governance Plan – The national governance plan should identify national stakeholder groups, roles and responsibilities, authority levels, national NG911 system oversight responsibility, and a model for interstate agreements. The national governance plan should be developed and implemented in the Foundational through Intermediate stages. In the End State stage, the national governance plan is reviewed and updated on a regular basis.

Functional & Technical Requirements	Specifications/Standards
Identify national stakeholders	• Report for National 9-1-1 Assessment Guidelines
Define roles and responsibilities of national-level stakeholders	• Report for National 9-1-1 Assessment Guidelines
Establish authority and responsibility for national-level oversight	• Report for National 9-1-1 Assessment Guidelines
Develop interstate agreement model	• NENA-INF-012.2-2015 – Inter-Agency Agreements Model Recommendations Information Document • SAFECOM Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials • TFOPA, WG2 Final Report, December 10, 2015
Review and update plans and agreements on a regular basis, at least annually	• Report for National 9-1-1 Assessment Guidelines • SAFECOM Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials

- Regularly Review National Governance Plan – The national governance plan should be reviewed and updated on a regular basis to reflect the current environment.

Functional & Technical Requirements	Specifications/Standards
Identify national stakeholders	• Report for National 9-1-1 Assessment Guidelines
Define roles and responsibilities of national-level stakeholders	• Report for National 9-1-1 Assessment Guidelines
Establish authority and responsibility for national-level oversight	• Report for National 9-1-1 Assessment Guidelines

Functional & Technical Requirements	Specifications/Standards
Develop interstate agreement model	• NENA-INF-012.2-2015 – Inter-Agency Agreements Model Recommendations Information Document • SAFECOM Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials • TFOPA, WG2 Final Report, December 10, 2015
Review and update plans and agreements on a regular basis, at least annually	• Report for National 9-1-1 Assessment Guidelines • SAFECOM Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials

A.1.1.5.   Procurement

The procurement of NG911 equipment, components, and services will be ongoing throughout the transition to NG911. Procurement will include an Emergency Services Internet Protocol network (ESInet), 911 call-handling equipment, recording and logging equipment, GIS and mapping services, Next Generation Core Services (NGCS), and possibly multiple levels of system management services.

A limitation of NGCS is the complexity and expense of deploying these systems. These limitations require small and rural 911 authorities to combine to create larger systems. NGCS are most efficiently and effectively deployed for regions with large populations, at a state level, or across a multistate region.[31] This limits 911 authorities in procuring and deploying their own autonomous NGCS.

---

[31] Task Force on Optimal PSAP Architecture, *Adopted Final Report,* (January 29, 2016), Federal Communications Commission, https://apps.fcc.gov/edocs_public/attachmatch/DA-16-179A2.pdf, page 148.

Functional & Technical Requirements	Specifications/Standards
Procurement of NG911 components at a state or regional level	• Applicable state or regional procurement laws • Code of Federal Regulations (CFR) Title 2, Part 200 – Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards

A.1.1.6.   Implementation

Implementation of NG911 equipment, components, and services will be ongoing throughout the transition to NG911. Implementation will include an ESInet, 911 call-handling equipment, recording and logging equipment, GIS and mapping services, NGCS, and possibly multiple levels of system management services.

Functional & Technical Requirements	Specifications/Standards
Implementation of NG911 equipment, components, and services	• NENA/APCO-REQ-001.1.1-2016 – Next Generation 9-1-1 Public Safety Answering Point Requirements • NENA Next Generation 9-1-1 Transition Policy Implementation Handbook • Applicable manufacturers' specifications • Applicable building, electrical, and grounding codes and standards

• Statewide Implementation Coordination – State-level oversight of implementation of NG911 equipment, components, and services. Systems integrator and statewide coordination and monitoring of implementation costs are included in this element.

Functional & Technical Requirements	Specifications/Standards
Implementation of NG911 equipment, components, and services	- NENA/APCO-REQ-001.1.1-2016 – Next Generation 9-1-1 Public Safety Answering Point Requirements - NENA Next Generation 9-1-1 Transition Policy Implementation Handbook - Applicable manufacturers' specifications - Applicable building, electrical, and grounding codes and standards

- Implementation Project Management – Technical project management will be required for implementation of NG911 equipment, components, and services. This project management may come from within state staff, or may need to be contracted from a third party.

Functional & Technical Requirements	Specifications/Standards
Implementation of NG911 equipment, components, and services	- NENA/APCO-REQ-001.1.1-2016 – Next Generation 9-1-1 Public Safety Answering Point Requirements - NENA Next Generation 9-1-1 Transition Policy Implementation Handbook - Applicable manufacturers' specifications - Applicable building, electrical, and grounding codes and standards

A.1.2. DATA DOMAIN

The Data Domain captures the data management responsibilities of PSAPs, regions, tribes, states, and national-level authorities as they prepare for and implement NG911. This domain includes a shift from tabular location data to full dependency on geographic information system data for the verification of caller location and routing of 911 calls. Activities related to this domain are illustrated in the matrix found in Figure A-2 below.
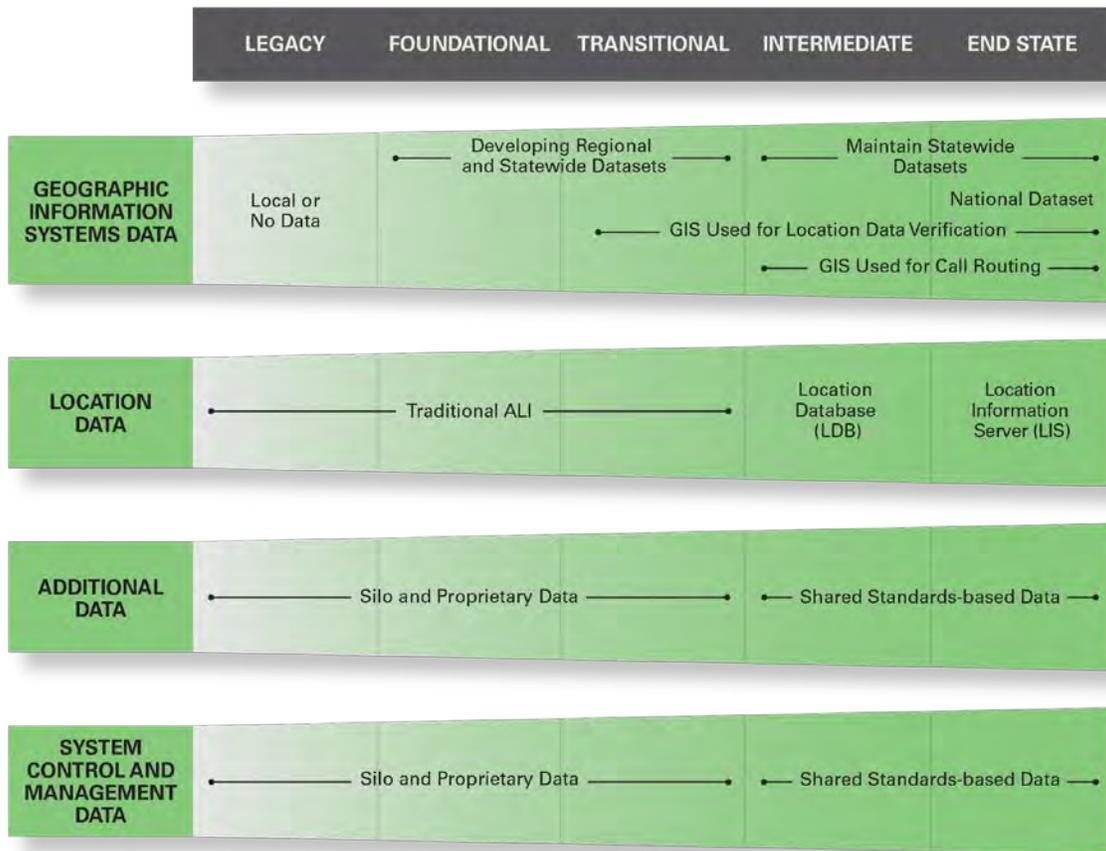
Figure A-2: NG911 Data Domain Matrix

A.1.2.1. *Geographic Information Systems Data*

GIS data represents local, regional, state, federal, and tribal jurisdictions, as well as location information, through a set of lines, polygons, and attributes. GIS data is layered to provide multiple sets of information for a single latitude and longitude location.

Many 911 authorities face a challenge in developing and maintaining their GIS data, which is a critical element to the proper function of NGCS. This challenge comes in multiple forms. The development and maintenance of GIS data requires specialized expertise and dedicated resources to support these functions. For many jurisdictions, these positions are filled by one or two people, if anyone at all. Local knowledge of the jurisdiction and region at large enable more precise data management. The combination of the critical role of these positions, the need for local knowledge, and limited staff make turnover in these positions a threat to operations.

Because NG911 relies on GIS data for call routing, the GIS data must be highly accurate. The PSAP or 911 authority responsible for the data must ensure that the data is of such quality to achieve a 98 percent or greater match rate with its legacy Master Street Address Guide (MSAG) and its GIS street centerline data before migrating to NG911. To accomplish this, the PSAP or 911 authority must have skilled GIS personnel on staff, or may elect to contract this task to a vendor that specializes in this type of work.

- Local or No Data – GIS data is not available or is locally managed, with little to no maintenance of the data set. GIS data has little to no correlation to automatic location identification (ALI) and MSAG data at the Legacy stage.

Functional & Technical Requirements	Specifications/Standards
Collecting and maintaining GIS data	• NENA 02-014 – GIS Data Collection and Maintenance Standards
Formatting GIS data to align with MSAG and ALI data	• NENA 02-010 – Standard Data Formats for 9-1-1 Data Exchange & GIS Mapping

- Developing Regional and Statewide Datasets – GIS data is being compared with MSAG and ALI datasets.[32] Regional and statewide data models are being developed for eventual use in validating caller location and call routing. Regional and statewide data is developed in the Foundational and Transitional stages.

---

[32] "Synchronizing GIS with MSAG & ALI," National Emergency Number Association, September 8, 2009, https://www.nena.org/?page=synch_gis_msag_ali.

Functional & Technical Requirements	Specifications/Standards
GIS data models for site/structure layers, boundaries, hydrology layer, cell site location layer, road centerlines, and other applicable datasets	• NENA-02-010 – Standard Data Formats For 9-1-1 Data Exchange & GIS Mapping[33]
Standardizing the synchronization of MSAG and ALI data with GIS road centerlines, site/structure data, and other related spatial data	• NENA 71-501 – Information Document for Synchronizing Geographic Information System Databases with MSAG & ALI
Correcting discrepancies between ALI, MSAG, and GIS data	• NENA 71-501 – Information Document for Synchronizing Geographic Information System Databases with MSAG & ALI

- GIS for Location Verification – GIS, ALI, and MSAG datasets are manipulated to enhance match rates. Data maintenance processes are developed and maintained. GIS data management processes may be at a stage that provides for caller location data to be verified to GIS data, as opposed to the traditional tabular MSAG data. Location validation is performed starting in the Transitional stage through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Required and optional GIS datasets; GIS data ownership, distribution and sharing of GIS data; quality assurance/quality control (QA/QC) recommendations	• NENA-STA-005.1-2017 – Standards for the Provisioning and Maintenance of GIS data to ECRFs/LVFs[34]
Address point placement guidelines and methodologies	• NENA-INF-014.1-2015 – Information Document for Development of Site/Structure Address Point GIS Data for 9-1-1
Location validation in transitional state	• NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document
Location Validation Function (LVF)	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)

---

[33] NENA-STA-006.1-201X – NG9-1-1 GIS Data Model – will replace this standard when complete.
[34] Emergency Call Routing Function (ECRF)/Location Validation Function (LVF)

Functional & Technical Requirements	Specifications/Standards
Location-to-Service Translation (LoST) protocol	• Internet Engineering Task Force (IETF) Request for Comments (RFC) 5222 – LoST: A Location-to-Service Translation Protocol
Universal Resource Identifier (URI)	• IETF RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax

- Maintain Developed Statewide Dataset – GIS data has 98 percent or greater match rate with the MSAG and ALI datasets.[35] Regional datasets, including all required boundary layers, have been coalesced into a congruent statewide dataset. GIS data is in the maintenance phase. A statewide data model is developed and available for use in validating caller location and call routing. Statewide data is established in the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
GIS data models for site/structure layers, boundaries, hydrology layer, cell site location layer, road centerlines, and other applicable datasets	• NENA-02-010 – Standard Data Formats For 9-1-1 Data Exchange & GIS Mapping[36]
Standardizing the synchronization of MSAG and ALI data with GIS road centerlines, site/structure data, and other related spatial data	• NENA 71-501 – Information Document for Synchronizing Geographic Information System Databases with MSAG & ALI
Correcting discrepancies between ALI, MSAG, and GIS data	• NENA 71-501 – Information Document for Synchronizing Geographic Information System Databases with MSAG & ALI

- GIS for Routing – GIS data and data maintenance processes have matured to the point that the dataset may be used for live 911 call routing. GIS data is now used for all location validation purposes. GIS routing is performed starting in the Intermediate stage through the End State stage.

---

[35] "Synchronizing GIS with MSAG & ALI," National Emergency Number Association, September 8, 2009, https://www.nena.org/?page=synch_gis_msag_ali.

[36] NENA-STA-006.1-201X – NG9-1-1 GIS Data Model – will replace this standard when complete.

Functional & Technical Requirements	Specifications/Standards
Presence Information Data Format – Location Object (PIDF-LO) protocol	• IETF RFC 3863 – Presence Information Data Format (PIDF) • IETF RFC 4119 – A Presence-based GEOPRIV[37] Location Object Format • IETF RFC 5139 – Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO) • IETF RFC 5491 – GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations
LoST protocol	• IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol
URI	• IETF RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax
Required and optional GIS datasets, GIS data ownership, distribution and sharing of GIS data, QA/QC recommendations	• NENA-STA-005.1-2017 – Standards for the Provisioning and Maintenance of GIS data to ECRFs/LVFs
Geospatial call routing with policy routing rules	• NENA-INF-011.1-2014 – NG9-1-1 Policy Routing Rules Operations Guide
Formatting location data and interchange of data between NG911 components	• NENA-STA-004.1.1-2014 – Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF) Standard
Spatial interface for data layer replication	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)

- <u>National GIS Dataset</u> – Statewide GIS data sets are coordinated with neighboring states to provide for a seamless national data set. GIS data is solely used for location validation and call routing. Nationwide data sets are available in the End State stage.

---

[37] Geographic Location/Privacy

Functional & Technical Requirements	Specifications/Standards
Seamless regional and national GIS dataset	• NENA-INF-009.1-2014 – Requirements for a National Forest Guide Information Document
LoST protocol	• IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol
URI	• IETF RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax
Location-to-Uniform Resource Locator (URL) mapping	• IETF RFC 5582 – Location-to-URL Mapping Architecture and Framework
Provisioning service boundaries and error reporting	• IETF RFC 6739 – Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol
Credential authentication	• International Telecommunication Union (ITU) Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks
Description of Forest Guide	• NENA-INF-009.1-2014 – Requirements for a National Forest Guide Information Document

A.1.2.2. Location Data

Location data involves the information and systems used to provide PSAPs and first responders with information regarding where an emergency may be found.

- Traditional ALI – Traditional ALI data is maintained for wireline and voice over IP (VoIP) callers. Wireless cellular tower address information is maintained in supplemental databases and queried for Phase I and Phase II location information. Traditional data is used from the Legacy stage through the Transitional stage. In the Legacy stage, location data is delivered over dedicated, point-to-point ALI circuits. In the Foundational stage, location data may now be delivered to PSAPs over an IP network, if such a network is in place. In the Transitional stage, location data may now be delivered to PSAPs over an IP network through a traditional ALI bid.

Functional & Technical Requirements	Specifications/Standards
Database management and quality measurements	• NENA 02-011, Version 7.1 – Data Standards for Local Exchange Carriers, ALI Service Providers & 9-1-1 Jurisdictions
ALI data formatting for Extensible Markup Language (XML) ALI queries	• NENA 04-005 – ALI Query Service Standard
ALI and MSAG data formatting	• NENA-02-010 – Standard Data Formats for 9-1-1 Data Exchange & GIS Mapping

- Location Database (LDB) – The LDB maintains traditional ALI data in conjunction with additional caller information. NG911 standards-based interfaces are used to retrieve location information at varying stages of call setup to enable an NG911 call flow.[38] The LDB is used in the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
Transitional location databases	• NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document
MSAG Conversion Service (MCS)	• NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document • NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)
PIDF-LO protocol	• IETF RFC 3863 – Presence Information Data Format (PIDF) • IETF RFC 4119 – A Presence-based GEOPRIV Location Object Format • IETF RFC 5139 – Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)

---

[38] "NG9-1-1 Transition Planning Considerations," National Emergency Number Association, November 20, 2013, http://www.nena.org/?page=NG911_TransitionPlng.

Functional & Technical Requirements	Specifications/Standards
PIDF-LO protocol (continued)	• IETF RFC 5491 – GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations
Processing legacy service provider's Service Order Input (SOI)	• NENA 02-011, Version 7.1 – Data Standards for Local Exchange Carriers, ALI Service Providers & 9-1-1 Jurisdictions
LoST protocol	• IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol
URI	• IETF RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax
HTTP-Enabled[39] Location Delivery (HELD) protocol	• IETF RFC 5985 – HTTP-Enabled Location Delivery (HELD)
Dereferencing location information via HELD	• IETF RFC 6753 – A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)
Transport Layer Security (TLS) protocol	• IETF RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2 (update draft in progress)
Emergency Service Protocol (E2)	• Telecommunications Industry Association (TIA)/Alliance for Telecommunications Industry Solutions (ATIS), J-STD-036-C – Enhanced Wireless 9-1-1 Phase II • NENA-05-001 – Implementation of the Wireless Emergency Service Protocol E2 Interface

- Location Information Server (LIS) – Location data is provided by an LIS using NG911 interfaces and protocols. The LIS is used in the End State stage.[40]

---

[39] Hypertext Transfer Protocol

[40] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, http://www.nena.org/?page=i3_Stage3.

Functional & Technical Requirements	Specifications/Standards
Validating locations stored in the LIS with LVF	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)
Conveying presence in the Session Initiation Protocol (SIP)	• IETF RFC 3856 – A Presence Event Package for the Session Initiation Protocol (SIP)
Control notifications, rate limits, and filters of LIS	• IETF RFC 3265 – Session Initiation Protocol (SIP) - Specific Event Notification • IETF RFC 6446 – Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control • IETF RFC 6447 – Filtering Location Notifications in the Session Initiation Protocol (SIP)
URI	• IETF RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax
HELD protocol	• IETF RFC 5985 – HTTP-Enabled Location Delivery (HELD)
Dereferencing location information via HELD	• IETF RFC 6753 – A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)
TLS protocol	• IETF RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2 (update draft in progress)
LIS requirements	• Telcordia GR-3158 – Generic Requirements for a Service Provider Location Information Server (LIS)
Credential authentication	• ITU Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks

A.1.2.3. Additional Data

Additional information regarding a call, caller, or location may be available to a call-taker and/or first responder to enhance situational awareness and improve emergency response.[41]

- Silo and Proprietary Data – Additional data may be available through disparate and proprietary systems offering little to no interoperability between PSAP 911 systems, such as call handling and computer-aided dispatch (CAD), within a PSAP and with other PSAPs. Examples of additional data in this stage include Advanced Automated Collision Notification (AACN) and personal safety applications with proprietary and/or Web-based interfaces. Silo systems exist from the Legacy stage through the Transitional stage.

Functional & Technical Requirements	Specifications/Standards
Additional information about the call, caller, or location	• NENA 71-001 – NENA Standard for NG9-1-1 Additional Data
XML data structure	• IETF (draft-ietf-ecrit-additional-data-38) – Additional Data Related to an Emergency Call (in development)
TLS protocol	• IETF RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2 (update draft in progress)
Additional Data Repository (ADR) interfaces and functionality	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)

- Shared Standards-based Data – Additional data may be accessed through standards-based interfaces and shared across multiple NG911 systems. PSAPs across a region or state may be able to access the same data where network connectivity and authorization is established. The examples of AACN and personal safety applications migrate from proprietary interfaces with limited access to standards-based data structures, such as XML, which are accessed by standards-based data-retrieval interfaces, such as HTTP GET, and secured by standards-based protocols such as TLS. Standards-based systems are implemented in the Intermediate stage through the End State stage.

---

[41] "NG9-1-1 Additional Data," National Emergency Number Association, September 17, 2009, https://www.nena.org/?page=NG911_AdditionalData.

Functional & Technical Requirements	Specifications/Standards
Additional information about the call, caller, or location	• NENA 71-001 – NENA Standard for NG9-1-1 Additional Data
XML data structure	• IETF (draft-ietf-ecrit-additional-data-38) – Additional Data Related to an Emergency Call (in development)
TLS protocol	• IETF RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2 (update draft in progress)
ADR interfaces and functionality	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)

A.1.2.4. *System Control and Management Data*

This refers to data related to the day-to-day control and management of NGCS. This data typically includes, but is not limited to, internal network element log files, network bandwidth utilization data, Simple Network Management Protocol (SNMP) traps, server operating system log files, data storage utilization, system access and session logs, failed login attempts, and password resets.

- Silo and Proprietary Data – The various systems operate in silos and do not share data or information.

Functional & Technical Requirements	Specifications/Standards
SNMP	• IETF RFC 3410 – Introduction and Applicability Statements for Internet Standard Management Framework • IETF RFC 3411 – An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks • IETF RFC 3412 – Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) • IETF RFC 3413 – Simple Network Management Protocol (SNMP) Applications

Functional & Technical Requirements	Specifications/Standards
SNMP (continued)	• IETF RFC 3414 – User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) • IETF RFC 3415 – View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) • IETF RFC 3416 – Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) • IETF RFC 3417 – Transport Mappings for the Simple Network Management Protocol (SNMP) • IETF RFC 3418 – Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
Syslog	• IETF RFC 5424 – The Syslog Protocol

- <u>Shared Standards-based Data</u> – The various systems share data and information to include Event Logging and Policy Routing Function (PRF) data.

  Event Logging data includes, but is not limited to, the time the call entered the network, which core components handled the routing, when the call was passed from one component to another, and whether the call was placed on hold, transferred, or conferenced with other agencies.

  PRF data is data describing the call-routing rules that agencies implement in the PRF functional element.

Functional & Technical Requirements	Specifications/Standards
End-to-end integrated logging	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)

Functional & Technical Requirements	Specifications/Standards
Recording of SIP traffic and media	• IETF RFC 7866 – Session Recording Protocol
Share data about emergencies between PSAPs	• APCO/NENA 2.105.1-2017 – NG9-1-1 Emergency Incident Data Document (EIDD)
PRF	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • NENA-STA-003.1.1-2014 – NENA Standard for NG9-1-1 Policy Routing Rules

Remainder of page is intentionally left blank.

A.1.3. APPLICATIONS AND SYSTEMS DOMAIN

The Applications and Systems Domain describes the applications, systems and other core functions of the NG911 systems. Activities related to this domain are illustrated in the matrix found in Figure A-3 below.

Figure A-3: NG911 Applications and Systems Domain Matrix

The NGCS is a collection of functional elements that each serve a role in routing a call to the proper PSAP. Each ESInet will have its own NGCS that will interoperate with neighboring NGCS to enable call and data transfer between PSAPs that are served by independent ESInets. Currently, the core services cannot operate independently without transitional components such as the gateways in the originating service environment (OSE).

The implementation of these systems is enabled by solution providers that have spent thousands of hours designing, developing, and testing their systems. ESInets and NGCS require sophisticated, complex software engineering that is integrated with VoIP network engineering. These NG911 service providers are required to enter into interconnection agreements with originating service providers (OSPs) and legacy 911 service providers to receive and transfer 911 calls.

911 authorities that choose to deploy a build, own, and operate model also need to enter into these same agreements. States and regions must assess their appetite for taking on the operational requirements and legal responsibilities for building, owning, and operating their own ESInet with NGCS. In many cases, the depth and breadth of expertise required to support this type of model often will sway a 911 authority to look at a services-based model. In these cases, a well-defined scope of work and a set of strong service level agreements (SLAs) provide 911 authorities with assurances for the level of service and extreme system availability required for public safety services.

A major driver for implementation of NGCS is that the systems are software-based and the requests for assistance are delivered to it over an IP network. These two characteristics provide great flexibility for accommodating future technologies as the 911 call continuum expands and new devices and services are introduced to the public. For example, the legacy 911 system cannot accommodate the delivery of health data available from medical sensors. In contrast, an ESInet powered by NGCS is able to support the delivery of this valuable data to telecommunicators and first responders. The flexible architecture of the NGCS will enable it to accommodate future generations of sensors and services as they enter the marketplace.

A.1.3.1.   Call Routing

Call-routing applications evaluate data contained in the call to determine the proper PSAP to receive that call. The existing Enhanced 911 (E911) systems use address data in tabular files to determine proper call routing. As 911 transitions to NG911, routing decisions will be based on geographic data contained in databases. In some cases, a 911 authority may move from the Legacy stage to the Intermediate stage without implementing the Foundational or Transitional stages.

- Trunk or Selective Routing – Routing is accomplished primarily through selective routing in communication service provider's (CSP's) tandem switches. In some cases, direct trunks are used between the CSP and PSAP. In either case, routing is based on tabular data files containing address and emergency service number (ESN) information. The ESN is mapped to a particular PSAP. Trunk or selective routing is performed in the Legacy stage.

Functional & Technical Requirements	Specifications/Standards
Selective routing	• NENA-03-005 – Generic Requirements for an Enhanced 9-1-1 Selective Routing Switch (archived)
Default routing functions	• NENA 03-008 – NENA Standard for Enhanced 9-1-1 (E9-1-1) Default Routing Assignments and Functions
Inter-tandem transfers	• NENA 03-003 – NENA Recommendation for the Implementation of Inter-Networking, E9-1-1 Tandem to Tandem

- IP Selective Routing – IP selective routing begins to replace circuit-switched legacy selective routing as calls are converted from Time Division Multiplexing (TDM) to VoIP. Routing information remains in a tabular file format. IP selective routing is performed in the Foundational stage and continues into the Transitional stage.

  Transitional components enable PSAPs and OSPs to migrate from the legacy environment to an NG911 environment without having to execute wholesale replacement of infrastructure. Deployment of an IP selective router (IPSR) is a transitional strategy that enables PSAPs to migrate to an ESInet while they develop their GIS data, staff, and operational processes to support the National Emergency Number Association (NENA) i3 location-validation and geospatial call-routing functions. While an IPSR is not a component within the NENA i3 NGCS, its position is the same as NGCS in a call flow.

  While IPSR solutions may provide a strategic advantage to PSAPs with limited GIS data, they are limited to legacy tabular-based routing rules that do not support advanced technologies such as sensor-based requests for assistance.

Functional & Technical Requirements	Specifications/Standards
Legacy Network Gateway (LNG)	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3265 – Session Initiation Protocol (SIP) - Specific Event Notification • NENA INF-008.2.1-2013 – NENA Transition Plan Considerations Information Document • IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol • Telcordia GR-3162 – Legacy Network Gateway Generic Requirements
IP selective routing	• NENA-03-005 – Generic Requirements for an Enhanced 9-1-1 Selective Routing Switch (archived)
Default routing functions	• NENA 03-008 – NENA Standard for Enhanced 9-1-1 (E9-1-1) Default Routing Assignments and Functions
IP call delivery in a transitional IPSR environment	• ATIS-0500019.2010 (R2015) – Request for Assistance Interface (RFAI) Specification
Inter-tandem transfers	• NENA 03-003 – NENA Recommendation for the Implementation of Inter-Networking, E9-1-1 Tandem to Tandem

- Geospatial Routing with Traditional Rules – Geospatial routing databases replace the tabular files used in call routing. Traditional rules-based routing, such as alternate and default routing, is implemented in the routing systems. Geospatial routing with traditional rules resides in the Intermediate stage.

  PSAPs may migrate directly to an ESInet with NGCS if they have the GIS data, staff, and processes in place. PSAPs that take this path will benefit from geospatial call routing, validating caller locations based on up-to-date GIS data, and the implementation of policy routing rules, which allows for more robust means to distribute call loads across a region. PSAPs that migrate directly to an i3 NGCS-based solution eliminate the eventual transition from an IPSR to an i3 NGCS, which will be required for those that first deploy an IPSR.

Functional & Technical Requirements	Specifications/Standards
LNG	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3265 – Session Initiation Protocol (SIP) - Specific Event Notification • NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document • IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol • Telcordia GR-3162 – Legacy Network Gateway Generic Requirements • IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol

Functional & Technical Requirements	Specifications/Standards
LNG (continued)	• IETF RFC 5985 – HTTP-Enabled Location Delivery (HELD) • NENA-05-001 – Implementation of the Wireless Emergency Service Protocol E2 Interface • NENA 04-005 – ALI Query Service Standard
Emergency Service Routing Proxy (ESRP)	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3265 – Session Initiation Protocol (SIP) - Specific Event Notification • IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol • IETF RFC 3863 – Presence Information Data Format (PIDF) • Telcordia GR-3157 – Emergency Services Routing Proxy (ESRP) Generic Requirements
PRF	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • NENA-STA-003.1.1-2014 – NENA Standard for NG9-1-1 Policy Routing Rules

Functional & Technical Requirements	Specifications/Standards
Emergency Call Routing Function (ECRF)	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3863 – Presence Information Data Format (PIDF)
LoST protocol	• IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol
URI	• IETF RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax
Spatial interface	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 6739 – Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol
Credential authentication	• ITU Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks

- Geospatial Routing with Progressive Rules – All NGCS are fully functional and all calls are routed based on geospatial data and a progressive set of configurable rules under the control of the PSAPs and 911 authorities. Geospatial and progressive rules-based routing is performed in the End State stage.[42]

Functional & Technical Requirements	Specifications/Standards
LNG	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

---

[42] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, http://www.nena.org/?page=i3_Stage3.

Functional & Technical Requirements	Specifications/Standards
LNG (continued)	• IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3265 – Session Initiation Protocol (SIP) – Specific Event Notification • NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document • IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol • Telcordia GR-3162 – Legacy Network Gateway Generic Requirements • IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol • IETF RFC 5985 – HTTP-Enabled Location Delivery (HELD) • NENA-05-001 – Implementation of the Wireless Emergency Service Protocol E2 Interface • NENA 04-005 – ALI Query Service Standard
ESRP	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP)

Functional & Technical Requirements	Specifications/Standards
ESRP (continued)	• IETF RFC 3265 – Session Initiation Protocol (SIP) – Specific Event Notification • IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol • IETF RFC 3863 – Presence Information Data Format (PIDF) • Telcordia GR-3157 – Emergency Services Routing Proxy (ESRP) Generic Requirements
PRF	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • NENA-STA-003.1.1-2014 – NENA Standard for NG9-1-1 Policy Routing Rules
ECRF	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3863 – Presence Information Data Format (PIDF)
LoST protocol	• IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol
URI	• IETF RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax
Spatial interface	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 6739 – Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol
Credential authentication	• ITU Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks

A.1.3.2. *Call-Handling Systems*

Call-handling systems connect the call to a telecommunicator, who then gathers the information from the caller and relays that information to responding agencies. Legacy call-handling systems are referred to as customer premises equipment (CPE); they handle only voice calls and receive those calls via analog trunks. IP-capable systems accept calls from direct SIP connections and, with the proper software, may accept multiple call types. Ancillary systems also may require upgrades to be compatible with NG911 call-handling systems. Such ancillary systems include but are not limited to, CAD, management information systems (MIS), and records management systems (RMS).

As the public switched telephone network (PSTN) migrates to an IP-based system, outside call centers such as poison control, language lines, N-1-1, and others will require upgrades to their systems and infrastructure to handle SIP calls. In the transition period, gateways may be required to connect these outside call centers.

The implementation of the NG911 and IP-based networks enables native integration of new devices and services into the NG911 system. Examples include, but are not limited to, alarms, sensors, and other future IP-based devices and services.

Service providers are implementing IP Multimedia Subsystems (IMS) in their networks as a means of delivering multimedia traffic across many different device types. IMS makes use of many of the IETF RFCs related to IP multimedia, including SIP. Because individual vendors interpret standards differently, SIP may not line up exactly in terms of what is implemented in IMS and that which is used in the i3 environment. Service providers may incur costs associated with transcoding SIP messaging exchanged between IMS and i3-compliant systems.

Although SIP is defined in IETF standards, each vendor has its own interpretation of the standards. What one sees as mandatory, another sees as optional. Incompatibilities will exist between versions of SIP implemented both by service providers and by 911 authorities. Workarounds will need to be implemented to overcome these discrepancies in standards interpretations.

- Legacy CPE – Equipment is capable only of processing voice calls. Primarily an analog 911 system, some later releases of CPE software may support early implementations of SIP call delivery, such as RFAI. A legacy PSAP gateway (LPG) is required to connect CPE to an ESInet for SIP call delivery. Legacy CPE will exist through the Transitional stage.

Functional & Technical Requirements	Specifications/Standards
CPE	• NENA 04-001 – NENA Recommended Generic Standards for E9-1-1 PSAP Equipment • NENA-04-004 – NENA Recommended Generic Standards for E9-1-1 PSAP Intelligent Workstations • ATIS-0500019.2010 (R2015) – Request for Assistance Interface (RFAI) Specification
LPG	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3265 – Session Initiation Protocol (SIP) – Specific Event Notification • NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document • IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol

- IP-based Call Handling System – IP-based systems are capable of direct SIP delivery of calls, and may accept any valid SIP call type that may be implemented in the application software. As new call types are developed, the call-handling system can be upgraded through software releases to accept and process the new call types. IP-based call-handling systems will appear in the Intermediate stage and continue through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Call-handling system	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3265 – Session Initiation Protocol (SIP) - Specific Event Notification • IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol • IETF RFC 3863 – Presence Information Data Format (PIDF) • Telcordia GR-3157 – Emergency Services Routing Proxy (ESRP) Generic Requirements • IETF RFC 5985 – HTTP-Enabled Location Delivery (HELD) • IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol • IETF RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax

A.1.3.3. Location Validation

Location validation checks the address to an authoritative dataset to verify the validity of the call location. The dataset is a tabular file in the legacy environment and a true relational database in the NG911 environment. In some cases, a 911 authority may move from the Legacy stage to the Intermediate stage without implementing the Foundational or Transitional stages.

Another limitation within the OSE concerns the current location-acquisition processes for wireless callers. NG911 provides the ability to route calls to the proper PSAP based on the location of the caller at the time the call was made. This is a significant improvement compared with today's legacy call-routing process; however, current location-acquisition technologies used for locating wireless callers require a substantial amount of time to provide a Phase II location.

In November 2013, Verizon reported that only 65 percent of calls were able to obtain a Phase II fix within 13 seconds, and 99 percent of calls were able to obtain a Phase II fix within 25 seconds.[43] This and other data contributed to the Federal Communications Commission's (FCC) update of the location accuracy rules in April 2015 to include a Time to First Fix (TTFF) of 30 seconds.[44] When every second counts, it is not reasonable to hold a call for 30 seconds to obtain a Phase II location in order to determine the appropriate route.

Consequently, wireless calls, which make up 76 percent of 911 calls,[45] will not be able to benefit from NG911's enhanced ability to accurately locate 911 callers until improvements are made to location-acquisition systems and processes.

- MSAG Validation – Location validation is performed using an MSAG tabular file. MSAG validation is performed in the Legacy stage and continues through the Transitional stage.

Functional & Technical Requirements	Specifications/Standards
MSAG data exchange format	- NENA 02-010 – NENA Standard Data Formats for 9-1-1 Data Exchange & GIS Mapping
MSAG development and maintenance	- NENA 02-011, Version 7.1 – NENA Data Standards for Local Exchange Carriers, ALI Service Providers & 9-1-1 Jurisdictions

---

[43] "Workshop On E911 Phase II Location," Verizon Wireless, https://transition.fcc.gov/bureaus/pshs/911/Phase%202/Workshop_11_2013/VZW_E911_Location_Overview_Nov2013.pdf.

[44] "Wireless E911 Location Accuracy Requirements," Federal Register, March 4, 2015, https://www.federalregister.gov/articles/2015/03/04/2015-04424/wireless-e911-location-accuracy-requirements#h-7.

[45] National 911 Program, *2015 National 911 Progress Report,* (February 2016), http://www.911.gov/pdf/National-911-Program-2015-ProfileDatabaseProgressReport-021716.pdf.

- Geospatial Validation – Geospatial validation is implemented to validate the location data from the CSP. Geospatial validation is performed from the Intermediate stage through the End State stage.[46]

Functional & Technical Requirements	Specifications/Standards
LVF	- NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) - IETF RFC 5985 – HTTP-Enabled Location Delivery (HELD) - IETF RFC 3693 – Geopriv Requirements - IETF RFC 4119 – A Presence-based GEOPRIV Location Object Format - IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol - IETF RFC 3863 – Presence Information Data Format (PIDF)
LoST protocol	IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol
Best practices for revalidating location	IETF RFC 6881 – Best Current Practice for Communications Services in Support of Emergency Calling
Credential authentication	ITU Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks

A.1.3.4.   Location Delivery

The location of a caller is provided to the PSAP to enable the dispatching of emergency services to the accurate location. Location delivery will move from a database bid after call delivery in a legacy environment to being delivered with the call in the Intermediate and End State stages. In some cases, a 911 authority may move from the Legacy stage to the Intermediate stage without implementing the Foundational or Transitional stages.

---

[46] "NG9-1-1 Transition Planning Considerations," National Emergency Number Association, November 20, 2013, http://www.nena.org/?page=NG911_TransitionPlng.

One major change in the NG911 environment concerns delivery of the location information. This information currently is delivered via an ALI bid after the call is answered. In the NG911 environment, the location information is delivered in the SIP headers with the call, although the location still can be updated by the call-taker during the call. Service providers will be required to develop and manage their own LIS to provide the location information in the initial call, and to provide updates during the call.

- Post Call Delivery over Dedicated ALI Circuits – The PSAP must query a database over serial data circuits and receive a response to obtain the ALI information after the call is received at the PSAP. Post call delivery over dedicated ALI circuits is performed in the Legacy stage.

Functional & Technical Requirements	Specifications/Standards
ALI bid	• NENA 04-005 – ALI Query Service Standard

- Post Call Delivery over Dedicated IP Circuits – The delivery of legacy ALI data and NG911 location data will continue as PSAPs transition to NG911. The implementation of IP-based delivery methods over dedicated IP circuits will reduce circuit costs. Delivery over IP exists in the Foundational stage.

Functional & Technical Requirements	Specifications/Standards
ALI bid	• NENA 04-005 – ALI Query Service Standard

- Delivery over IP Circuits – The delivery of legacy ALI data and NG911 location data will continue as PSAPs transition to NG911. The implementation of IP-based delivery methods over the ESInet will reduce circuit costs. Delivery over IP exists in Transitional stage.

Functional & Technical Requirements	Specifications/Standards
ALI bid	• NENA 04-005 – ALI Query Service Standard

- <u>Delivery by PIDF-LO in SIP Header</u> – NG911 location information is encapsulated in the PIDF-LO and included in the SIP header as part of the call setup. PIDF-LO is used in the Intermediate and End State stages.[47]

Functional & Technical Requirements	Specifications/Standards
PIDF-LO in the SIP header	- NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) - NENA 08-752 – NENA Technical Requirements Document for Location Information to Support IP-Based Emergency Services - IETF RFC 3863 – Presence Information Data Format (PIDF)

A.1.3.5. *Call Processing*

Call-processing equipment processes the information from the call and delivers it to the responders in the field. Call-processing equipment includes CAD systems and mobile data systems.

- <u>Silo and Proprietary Systems</u> – Call-processing equipment has proprietary systems and interconnections. These systems will exist from the Legacy stage through the Transitional stage.

Functional & Technical Requirements	Specifications/Standards
Input data from call-handling systems	- NENA 04-001 – NENA Recommended Generic Standards for E9-1-1 PSAP Equipment - NENA 04-005 – ALI Query Service Standard - NENA 02-010 – Standard Data Formats for 9-1-1 Data Exchange & GIS Mapping
Output information to responders	Proprietary systems

---

[47] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, http://www.nena.org/?page=i3_Stage3.

- Standards-based Systems – The systems use open standards that permit data sharing between diverse NG911 systems. Standards-based systems will appear in the Intermediate stage and continue through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Input data from call-handling systems	- National Information Exchange Model (NIEM) - NENA 04-004 – NENA Recommended Generic Standards for E9-1-1 PSAP Intelligent Workstations - NENA 04-501 – Integrating Applications on Intelligent Workstations Technical Information Document
Output information to responders	National Information Exchange Model (NIEM)

A.1.3.6.   *Event Logging*

Event logging is the capture and storage of all information related to a given call. This includes, but is not limited to, the time the call entered the network, which core components handled the routing, when the call was passed from one component to another, and whether the call was placed on hold, transferred, or conferenced with other agencies. It is a complete record of how the call was handled.[48]

- Silo and Proprietary Data in Separate Systems – Each disparate system maintains its own logging of events, creating silos of information. Compilation of data between systems and various system operators to form a complete picture can be tedious. Silo and proprietary systems are in place from the Legacy stage to the Transitional stage.

Functional & Technical Requirements	Specifications/Standards
Logging performed independently by each NG911 system	Individual system specifications

---

[48] Ibid.

- End-to-End Integrated Logging – The logging of information is consolidated, reported to, or accessible from a system that can compile all information for a single call into a single log for troubleshooting or monitoring. End-to-end logging is implemented in the Intermediate stage and continues into the End State stage.

Functional & Technical Requirements	Specifications/Standards
End-to-end integrated logging	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)
Recording of SIP traffic and media	• IETF RFC 7866 – Session Recording Protocol
Sharing of data about emergencies between PSAPs	• APCO/NENA 2.105.1-2017 – NG9-1-1 Emergency Incident Data Document (EIDD)
Credential authentication	• ITU Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks

A.1.3.7.   Data Analytics

Data analytics currently present a challenge because of the proprietary and siloed nature of the components comprising the present 911 system. NG911 may bring a large amount of data to the public safety system. Getting the right data to the right people at the right time will enhance the NG911 system. Data analytics provide a means for the NG911 system to process large amounts of data based on the needs of the system participants. Data analytics also refer to the statistical processing of data collected in the event-logging systems to detect trends, anomalies and, potentially, problems.

- Automated Data Analytics – The users, governing body, state, or 911 authorities will develop or adopt standards and procedures for data analytics. With standards-based logging and additional data sources implemented in all NG911 systems, data can be analyzed to reduce the information presented to the PSAP or passed directly to responders, to make better routing decisions and to provide better service to the public. Automatic data analytics begins in the Intermediate stage and continues into the End State stage.

Functional & Technical Requirements	Specifications/Standards
Data QA	• NENA 02-014 – GIS Data Collection and Maintenance Standards
Identify data sources and uses of that data	• Local system access • Local policy and procedures
Develop algorithms to process data	• Data-specific needs • Data providers' permissions
Review and update processes and procedures based on use	• Local policy and procedures • Local needs
Logged-data requirements	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)
Credential authentication	• ITU Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks

A.1.3.8. *Forest Guide*

The Forest Guide is a database of geographic data used to route calls to the proper PSAP. The Forest Guide will be implemented at national and state levels with access by regional, state, and local entities.[49] Each successive level will have more-precise geographic information.

- Forest Guide in Place – Geographic data is coalesced at each successive level and a Forest Guide is implemented to allow for more-precise routing between regional and state-level ESInets. The Forest Guide is implemented in the Intermediate stage and continues into the End State stage.

Functional & Technical Requirements	Specifications/Standards
Role of the Forest Guide	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)
Forest Guide requirements	• NENA-INF-009.1-2014 – Requirements for a National Forest Guide Information Document
Architecture of hierarchical lookup systems	• IETF RFC 5582 – Location-to-URL Mapping Architecture and Framework

---

[49] "Requirements for a National Forest Guide," National Emergency Number Association, August 14, 2014, https://www.nena.org/?NatlForestGuide.

Functional & Technical Requirements	Specifications/Standards
LoST protocol	• IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol
GIS layer synchronization	• IETF RFC 6739 – Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol
Credential authentication	• ITU Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks

- <u>National Level Forest Guide in Place</u> – Geographic data is coalesced at each successive level and a national-level Forest Guide is implemented to allow for routing between regional and state-level ESInets. The national-level Forest Guide is implemented in the End State stage.

Functional & Technical Requirements	Specifications/Standards
Role of the Forest Guide	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)
Forest Guide requirements	• NENA-INF-009.1-2014 – Requirements for a National Forest Guide Information Document
Architecture of hierarchical lookup systems	• IETF RFC 5582 – Location-to-URL Mapping Architecture and Framework
LoST protocol	• IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol
GIS layer synchronization	• IETF RFC 6739 – Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol
Credential authentication	• ITU Recommendation X.509 – The Directory: Public-key and attribute certificate frameworks

A.1.4. INFRASTRUCTURE DOMAIN

The Infrastructure Domain describes the infrastructure elements that interconnect NGCS of the Applications and Systems Domain. Activities related to this domain are illustrated in the matrix found in Figure A-4 below.
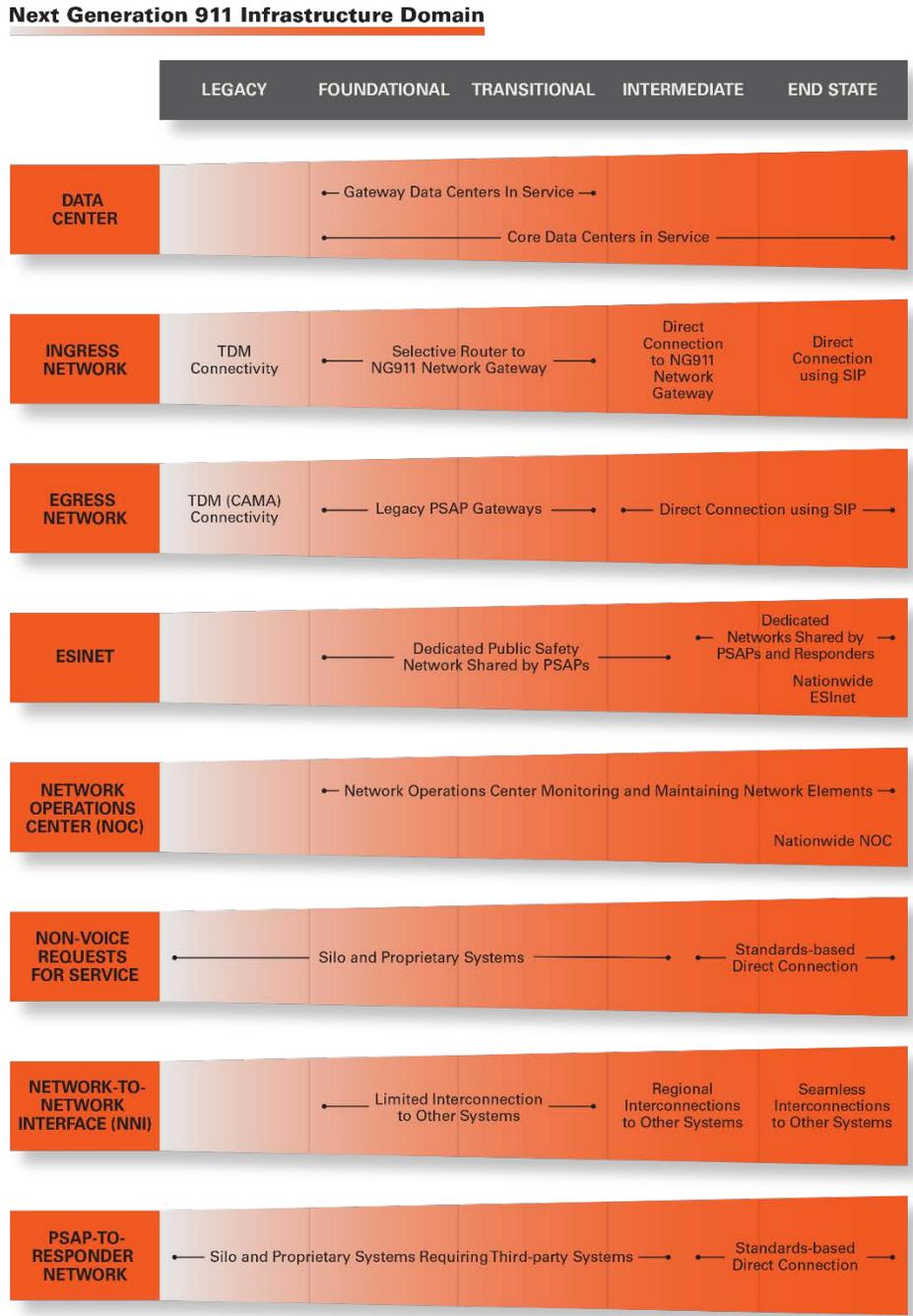
Figure A-4: NG911 Infrastructure Domain Matrix

Today, IPSRs, NGCS, and their security components are found in local, regional, and state pockets of deployment across the country, hence proving technical feasibility. The implementation of these systems is enabled by solution providers that have spent thousands of hours designing, developing, and testing their systems. ESInets and NGCS require sophisticated, complex software engineering that is integrated with VoIP network engineering. These NG911 service providers are required to enter into interconnection agreements with OSPs and legacy 911 service providers to receive and transfer 911 calls.

911 authorities that choose to deploy a build, own, and operate model also need to enter into these same agreements. States and regions must assess their appetite for taking on the operational requirements and legal responsibilities for building, owning, and operating their own ESInet with NGCS. In many cases, the depth and breadth of expertise required to support this type of model often will sway a 911 authority to look at a services-based model. In these cases, a well-defined scope of work and a set of strong SLAs provide 911 authorities with assurances for the level of service and extreme system availability required for public safety services.

Transitional components enable PSAPs to migrate from the legacy environment to an NG911 environment without having to execute wholesale replacement of infrastructure. Deployment of an IPSR is a transitional strategy that enables PSAPs to migrate to an ESInet while they develop their GIS data, staff, and operational processes to support the NENA i3 location validation and geospatial call-routing functions. While an IPSR is not a component within the NENA i3 NGCS, its position is the same as NGCS in a call flow.

A.1.4.1.   Data Center

Data centers contain many types of NG911 systems and equipment.

- Gateway Data Centers – During the course of NG911 implementation, gateways will be hosted in data centers to support the NG911 call flow. These may or may not be colocated with the NGCS. Gateways convert TDM voice calls to SIP for transport across the ESInet. There are three types of gateways: LNGs, legacy selective router gateways (LSRGs), and LPGs. Gateways will be implemented in the Foundational stage and continue to operate through the majority of the Transitional stage; gateways should be decommissioned by the end of the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
Data centers	• TIA-942-A – Telecommunications Infrastructure Standard for Data Centers • TIA-606-B – Administration Standard for Telecommunications Infrastructure
LNG	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3265 – Session Initiation Protocol (SIP) - Specific Event Notification • NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document • IETF RFC 3550 – RTP: A Transport Protocol for Real-Time Applications • IETF RFC 6442 – Location Conveyance for the Session Initiation Protocol • Telcordia GR-3162 – Legacy Network Gateway Generic Requirements • IETF RFC 5222 – LoST: A Location-to-Service Translation Protocol • IETF RFC 5985 – HTTP-Enabled Location Delivery (HELD) • NENA-05-001 – Implementation of the Wireless Emergency Service Protocol E2 Interface

Functional & Technical Requirements	Specifications/Standards
LNG (continued)	• NENA 04-005 – ALI Query Service Standard
Signaling System 7 (SS7) call delivery to LNGs	• Telcordia GR-2956 – CCS/SS7 Generic Requirements in Support of E9-1-1 Service
LSRG	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • Telcordia GR-3170 – Legacy Selective Router (SR) Gateway Generic Requirements

- Core Data Centers – NGCS data centers host the equipment for security and call-routing functions related to emergency calls, regardless of the incoming call type (e.g., voice, text, multimedia, telematics). NGCS systems are software-driven, requiring highly available servers. These servers must reside in secure, redundant, and resilient data centers. Core data centers will be implemented in the Foundational stage and continue through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Data centers	• TIA-942-A – Telecommunications Infrastructure Standard for Data Centers • TIA-606-B – Administration Standard for Telecommunications Infrastructure

A.1.4.2. Ingress Network

Ingress networks deliver the incoming calls (e.g., voice, text, multimedia, telematics) to the ESInet. The migration to NG911 will require service providers to make changes in the OSE. Service providers must migrate from the current TDM call-delivery environment to SIP delivery over IP networks. Service providers slowly are moving from the legacy PSTN Class 5 switches to IP-based soft switches using SIP signaling to deliver calls. During the transition period, service providers will need to implement LNGs to translate the TDM circuits to SIP for delivery across the ESInet. Once the transition of the OSE is complete, the gateway functionality will be decommissioned, though the physical devices likely will remain in service, performing other vital network functions.

- TDM Connectivity – TDM connectivity delivers calls to the legacy selective routers located at CSP central offices. Centralized automatic message accounting (CAMA) trunks deliver TDM voice calls and their associated automatic number identification (ANI) data from the selective routers to the PSAPs. TDM connectivity is a Legacy stage technology.

Functional & Technical Requirements	Specifications/Standards
TDM connectivity between the selective router and/or LNG with legacy PSAP equipment	- Telcordia GR-2953-CORE – Enhanced MF Signaling: E9-1-1 Tandem to PSAP Interface - NENA 03-002 – NENA Standard for the Implementation of Enhanced MF Signaling, E9-1-1 Tandem to PSAP - NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document
SS7 TDM connectivity between OSE to selective router and/or LNG	Telcordia GR-2956 – CCS/SS7 Generic Requirements in Support of E9-1-1 Service

- Selective Router to NG911 Gateway – Voice calls are delivered from the legacy selective routers in the OSE to LNGs and LSRGs via multifrequency (MF) or SS7 trunks for conversion to VoIP signaling and media. Call delivery from selective routers to NG911 gateways is performed in the Foundational stage through the Transitional stage.[50]

Functional & Technical Requirements	Specifications/Standards
Selective router to NG911 gateway	- NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) - NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document
SS7 TDM connectivity between selective router and/or LNG	Telcordia GR-2956 – CCS/SS7 Generic Requirements in Support of E9-1-1 Service

---

[50] "NG9-1-1 Transition Planning Considerations," National Emergency Number Association, November 20, 2013, http://www.nena.org/?page=NG911_TransitionPlng.

- Direct Connection to NG911 Gateway – Selective routers and CAMA trunks are phased out in favor of direct connections from CSP central offices to the LNGs. Voice calls are delivered from the OSE to LNGs and LSRGs via MF or SS7 trunks for conversion to VoIP signaling and media. Text and other non-voice call types are delivered via IP connections from the CSPs to the Border Control Function (BCF) at the edge of the ESInet. Direct connection from the OSE to the NG911 gateways is performed in the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
Direct connection to NG911 gateway	- NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) - Telcordia GR-2956 – CCS/SS7 Generic Requirements in Support of E9-1-1 Service - NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document

- Direct SIP Connections – All emergency calls, regardless of type, are delivered from the OSE to the BCF at the edge of the ESInet.

Functional & Technical Requirements	Specifications/Standards
Direct SIP connections	- NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) - NENA 08-506 – NENA Emergency Services IP Network Design for NG9-1-1 (NID) (including subsequent versions) - IETF RFC 3261 – SIP: Session Initiation Protocol - IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) - IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers - IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP)

Functional & Technical Requirements	Specifications/Standards
Direct SIP connections (continued)	• IETF RFC 3265 – Session Initiation Protocol (SIP) – Specific Event Notification • IETF RFC 5411 – A Hitchhiker's Guide to the Session Initiation Protocol (SIP)

A.1.4.3.   Egress Network

The egress networks connect traffic from the NGCS to legacy PSAPs and to non-911 systems and PSAP networks, which enables legacy PSAPs to receive calls from the NGCS and other PSAPs, and to conference in or transfer calls to third parties outside the NG911 system. Two examples of third parties are language lines and poison-control centers. The legacy network uses administrative lines to connect to agencies via ten-digit dialing. Connections to other PSAPs on the same selective router are handled with star (*) or pound (#) codes across the CAMA trunks.

As the PSTN migrates to an IP-based system, third-party call centers will require upgrades to their systems and infrastructure to handle SIP calls. In the transition period, gateways may be required to connect the third-party call centers.

The implementation of the NG911 and IP-based networks enables native integration of new devices and services into the NG911 system. Examples include, but are not limited to, alarms, sensors, and other future IP-based devices and services.

- TDM Connectivity – TDM connectivity to the legacy tandems located at CSP central offices exists to provide legacy telephone connectivity for outbound calls and to allow conferencing with outside agencies, such as a language service or poison control. CAMA trunks enable the transfer of 911 voice calls and their associated ANI data back through the selective routers to other PSAPs. TDM connectivity is a Legacy stage technology.

Functional & Technical Requirements	Specifications/Standards
TDM connectivity between the selective router and/or LNG and/or legacy PSAP	• Telcordia GR-2953-CORE – Enhanced MF Signaling: E9-1-1 Tandem to PSAP Interface • NENA 03-002 – NENA Standard for the Implementation of Enhanced MF Signaling, E9-1-1 Tandem to PSAP

Functional & Technical Requirements	Specifications/Standards
TDM connectivity between the selective router and/or LNG and/or legacy PSAP (continued)	• NENA-INF-008.2-2013 – NENA NG9-1-1 Transition Plan Considerations Information Document
SS7 TDM connectivity between OSE to selective router and/or LNG and/or legacy PSAP	• Telcordia GR-2956 – CCS/SS7 Generic Requirements in Support of E9-1-1 Service

• Legacy PSAP Gateway – Legacy PSAPs connected to the NGCS will use LPGs to convert VoIP calls to TDM. Similarly, outbound VoIP-to-TDM trunks are provisioned on the LNGs and LSRGs to handle calls from the ESInet back into the legacy TDM network. Legacy gateways are provisioned in the Foundational stage through the Transitional stage. The LPGs will be removed by the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
LPG	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • Telcordia GR-3166 – Legacy Public Safety Answering Point (PSAP) Gateway Generic Requirements

• PSAP Direct/Outbound Gateways – PSAP equipment is directly connected and processing all traffic in IP and SIP. Outbound VoIP-to-TDM trunks remain provisioned on the LNGs and LSRGs to handle calls from the ESInet back into the legacy TDM network. PSAPs are connected via SIP, but outbound gateways remain in the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
PSAP direct/outbound gateways	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)
LSRG	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • Telcordia GR-3170 – Legacy Selective Router (SR) Gateway Generic Requirements

- Direct Connection via SIP – All outbound calls will be handled on VoIP trunks through the BCF. Gateways no longer will be required in the End State stage.

Functional & Technical Requirements	Specifications/Standards
Direct connection via SIP	- NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) - NENA 08-506 – NENA Emergency Services IP Network Design for NG9-1-1 (NID) (including subsequent versions) - IETF RFC 5411 – A Hitchhiker's Guide to the Session Initiation Protocol (SIP)

The speed with which service providers are migrating their networks from TDM to SIP delivery varies widely. Even a given service provider may be moving at different paces within their network. Many regional and local carriers already have made the move to softswitches and VoIP, but are converting their 911 calls to TDM and passing the calls to the incumbent local exchange carrier (ILEC) for aggregation.

Although SIP is defined in IETF standards, each vendor has its own interpretation of the standards. What one sees as mandatory, another sees as optional. Incompatibilities will exist between versions of SIP implemented both by service providers and by 911 authorities. Workarounds will need to be implemented to overcome these discrepancies in standards interpretations.

A.1.4.4. ESInet

The ESInet is the underlying IP network, built to public safety-grade standards, which supports the systems and services required to deliver calls to the PSAPs. Although broadband is considered widely deployed, there are areas in the country where it either is not deployed, or is deployed but with bandwidth limitations. The limitations may be due to distance, loop quality, or other factors.

- Dedicated Network for PSAPs – Local, regional, and state ESInets are designed, built, and tested. NGCS are installed, configured, and tested across the ESInets. Live 911 calls now traverse the ESInet for delivery to PSAPs. Independent ESInets are deployed in the Foundational stage and remain through the Intermediate stage.

Functional & Technical Requirements	**Specifications/Standards**
Dedicated network for PSAPs	• NENA 08-506 – NENA Emergency Services IP Network Design for NG9-1-1 (NID) (including subsequent versions) • IETF RFC 2328 – OSPF Version 2 • IETF RFC 5340 – OSPF for IPv6 • IETF RFC 5880 – Bidirectional Forwarding Detection (BFD) • IETF RFC 5881 – Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop) • IETF RFC 5882 – Generic Application of Bidirectional Forwarding Detection (BFD) • IETF RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers • IETF RFC 2475 – An Architecture for Differentiated Services • IETF RFC 5411 – A Hitchhiker's Guide to the Session Initiation Protocol (SIP)

- Interconnected Networks – Local, regional, and state ESInets are interconnected and permit other public safety traffic in addition to 911 calls, such as shared incident data and radio traffic. Interconnected ESInets will begin to appear early in the Intermediate stage, but are complete in the End State stage.

Functional & Technical Requirements	**Specifications/Standards**
Interconnected networks	• NENA 08-506 – NENA Emergency Services IP Network Design for NG9-1-1 (NID) (including subsequent versions) • ATIS-0300104 – Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability • IETF RFC 4271 – A Border Gateway Protocol 4 (BGP-4) • IETF RFC 2328 – OSPF Version 2 • IETF RFC 5340 – OSPF for IPv6 • IETF RFCs 5880 – Bidirectional Forwarding Detection (BFD) • IETF RFC 5881 – Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop) • IETF RFC 5882 – Generic Application of Bidirectional Forwarding Detection (BFD) • IETF RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers • IETF RFC 2475 – An Architecture for Differentiated Services • Telcordia GR-3112 – Emergency Services Network Interconnection

- Nationwide ESInet – The regional and state ESInets need access to a higher-level network to reach agencies outside their area. The nationwide ESInet will be the network-of-networks that integrates and interconnects the state and regional ESInets, and will exist in the End State stage.

Functional & Technical Requirements	Specifications/Standards
Nationwide ESInet	• NENA 08-506 – NENA Emergency Services IP Network Design for NG9-1-1 (NID) (including subsequent versions) • ATIS-0300104 – Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability • IETF RFC 4271 – A Border Gateway Protocol 4 (BGP-4) • IETF RFC 2328 – OSPF Version 2 • IETF RFC 5340 – OSPF for IPv6 • IETF RFCs 5880 – Bidirectional Forwarding Detection (BFD) • IETF RFC 5881 – Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop) • IETF RFC 5882 – Generic Application of Bidirectional Forwarding Detection (BFD) • IETF RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers • IETF RFC 2475 – An Architecture for Differentiated Services • Telcordia GR-3112 – Emergency Services Network Interconnection

A.1.4.5.   *Network Operations Center (NOC)*

The ESInet and NGCS are secured through multiple components and system configurations. These components include firewalls, session border controllers (SBCs), intrusion-detection systems (IDSs), intrusion prevention systems (IPSs), and ICAM systems. These systems operate 24 hours a day, 7 days a week, 365 days a year (24 x 7 x 365) and are managed by a security operations center (SOC). In some cases, an NG911 service provider may consolidate these functions with its network operations center (NOC). The NOC/SOC provides constant monitoring of the ESInet and

NGCS, looking for anomalies and alarms. As incidents arise, the NOC/SOC is required to have standard operating procedures (SOPs) in place for notifying customers and the FCC Network Operations Reporting System (NORS). The NOC also originates and manages trouble tickets with the appropriate service provider or vendor, reports on the health of the networks and systems, and reports on trouble ticket resolution and status.

- NOC Network Monitoring – The NOC monitors networks for trouble and dispatches appropriate resources to resolve the problem. The NOC typically provides regular management reports regarding its activities. The NOC will be required to monitor and manage the ESInet from its initial installation through its lifetime. SLAs will govern problem severity, response times, and reporting. One or multiple NOCs will be deployed in the Foundational stage and continue through the End State stage.

Functional & Technical Requirements	Specifications/Standards
NOC monitoring network	- IETF RFC 3411 – An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks - IETF RFC 3412 – Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) - IETF RFC 3413 – Simple Network Management Protocol (SNMP) Applications - IETF RFC 3414 – User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) - IETF RFC 3415 – View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) - IETF RFC 3416 – Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) - IETF RFC 3417 – Transport Mappings for the Simple Network Management Protocol (SNMP)

Functional & Technical Requirements	Specifications/Standards
NOC monitoring network (continued)	• IETF RFC 3418 – Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) • Information Technology Infrastructure Library (ITIL) v3
Evaluating voice quality through mean opinion score (MOS)	• ITU-T Recommendation P.800.2 – Mean opinion score interpretation and reporting

- <u>National-level NOC</u> – The national-level NOC will have an overarching view of the networks at all levels, and will be able to advise subordinate NOCs of issues in their areas. The NOC typically provides regular management reports regarding its activities. SLAs will govern problem severity, response times, and reporting. The national-level NOC will be deployed in the End State stage.

Functional & Technical Requirements	Specifications/Standards
NOC monitoring network	• IETF RFC 3411 – An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks • IETF RFC 3412 – Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) • IETF RFC 3413 – Simple Network Management Protocol (SNMP) Applications • IETF RFC 3414 – User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) • IETF RFC 3415 – View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

Functional & Technical Requirements	Specifications/Standards
NOC monitoring network (continued)	• IETF RFC 3416 – Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) • IETF RFC 3417 – Transport Mappings for the Simple Network Management Protocol (SNMP) • IETF RFC 3418 – Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) • ITIL v3
Evaluating voice quality through MOS	• ITU-T recommendation P.800.2 – Mean opinion score interpretation and reporting

A.1.4.6.   Non-voice Requests for Service

Non-voice requests for service are machine-to-machine calls, such as those generated by alarm or telematics systems. These calls may be routed differently than a voice call. The implementation of NG911 and IP-based networks enables native integration of new devices and services into the NG911 system. Examples include, but are not limited to, alarms, sensors, and other future IP-based devices and services.

- Silo and Proprietary Systems – These call types typically are handled by a third-party system, such as a central station monitoring system or a call center, which then contacts the appropriate PSAP and relays the pertinent information. Silo and proprietary systems are in place in the Legacy stage and continue into the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
Silo and proprietary systems	• Individual system processes and procedures

- Shared Standards-based Connections – Proprietary systems are replaced by standards-based systems, and all non-voice requests for service are delivered via standards-based NG911 systems to the appropriate PSAP. Shared standards-based systems will begin deployment in the Intermediate stage and will continue through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Shared standards-based connections	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • ATIS-PP-0500002.2008 (R2013) – Emergency Services Messaging Interface (ESMI)
Non-human-initiated calls for service	• Organization for the Advancement of Structured Information Standards (OASIS, oasis-200402-cap-core-1.0) – Common Alerting Protocol v1.0 • OASIS (EDXL-DE v1.0) – Emergency Data Exchange Language Distribution Element (EDXL-DE) v1.0 • APCO/CSAA 2.101.2-2014 – Automated Secure Alarm Protocol (ASAP) • IETF RFC 3261 – SIP: Session Initiation Protocol • IETF RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3263 – Session Initiation Protocol (SIP): Locating SIP Servers • IETF RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3265 – Session Initiation Protocol (SIP) - Specific Event Notification • IETF (draft-ietf-ecrit-additional-data-38) – Additional Data Related to an Emergency Call (in development)

A.1.4.7.   Network-to-Network Interface (NNI)

The NNI connects disparate service providers' networks to each other, with appropriate safeguards at the interconnection point and within the respective systems to protect both networks. The NNI will be used between ESInets of different providers and states, but also between emergency service networks, additional data systems, and responder networks, to include the First Responder Network Authority (FirstNet) Nationwide Public Safety Broadband Network (NPSBN).

- Limited Interconnection – Service providers will implement IP connections between their respective data networks to allow traffic to flow from one network to another network. Interconnections may use proprietary interfaces and be limited in volume. Limited interconnection will be in place from the Foundational stage through the Transitional stage.

Functional & Technical Requirements	Specifications/Standards
Interconnection on a system-by-system basis	• Proprietary interconnection protocols

- Regional Interconnections – Interconnections between systems begin to expand and make use of standards-based NNI connections between service providers, NG911 systems, and their respective data networks, and allow standards-based traffic to flow from one network to another network. Regional interconnections will be in place during the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
Interconnection	• ATIS-1000026.2008 (R2013) – Session Border Controller Functions and Requirements • ATIS-1000029.2008 (R2013) – Security Requirements for NGN • ATIS-1000034.2010 (R2015) – Next Generation Network (NGN): Security Mechanisms and Procedures • ATIS-0300104 – Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability

Functional & Technical Requirements	Specifications/Standards
Interconnection (continued)	• Telcordia GR-3112 – Emergency Services Network Interconnection

- <u>Seamless Interconnection</u> – Seamless, standards-based NNI connections between the service providers, NG911 systems, responder networks, and their respective data networks allow standards-based traffic to flow from one network to another network. Seamless interconnection will exist in the End State stage.

Functional & Technical Requirements	Specifications/Standards
Seamless interconnection	• ATIS-1000026.2008 (R2013) – Session Border Controller Functions and Requirements • ATIS-1000029.2008(R2013) – Security Requirements for NGN • ATIS-1000034.2010 (R2015) – Next Generation Network (NGN): Security Mechanisms and Procedures • ATIS-0300104 – Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability • Telcordia GR-3112 – Emergency Services Network Interconnection

A.1.4.8.   PSAP-to-Responder Network

The PSAP-to-responder network transfers information from the PSAP to responders in the field. Migrating to NG911 will give PSAPs the ability to natively handle SIP voice, text, multimedia, machine-to-machine, and other IP-network-enabled call types. The any-to-any nature of IP networks also enhances the disaster-recovery options available to PSAPs. Implementing call-handling systems in a hosted model (e.g., colocated in data centers with NGCS) enables PSAPs to deploy resources anywhere they have access to a secure broadband connection. Using a specially configured and secured laptop, personnel can log into the hosted call-handling system and take calls as if they were in their normal PSAP.

The implementation of the NG911 environment and IP-based networks enables native integration of new devices and services into the NG911 system. Examples include, but are not limited to, alarms, sensors, and other IP-based devices and services that may be developed in the future. The move to NG911 is the first step in getting supplemental data to emergency responders via FirstNet's NPSBN.

- Silo and Proprietary Systems – Responder communications use locally or regionally controlled independent systems, such as land mobile radio (LMR) or mobile data terminals connected to a local CAD system. Silo systems are in place in the Legacy stage and will continue into the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
Legacy LMR	• 47 CFR Part 90 – Private Land Mobile Radio Services • TIA-102 Series – Telecommunications Land Mobile Communications (APCO/Project 25) ***Includes all current TIA/EIA TSB 102, TIA/EIA-102 AND TIA-102 Standards***
Commercial data services	• Vendor-specific protocols

- Shared Standards-Based System – PSAPs are connected to responders with standards-based systems that will allow information flow, such as the network envisioned by FirstNet. Limited information on the interconnection methods with the FirstNet network was available at the time of this report. Shared NG911 systems will be implemented beginning in the Intermediate stage and will be completed in the End State stage.

Functional & Technical Requirements	Specifications/Standards
Shared standards-based system	• ATIS-1000061.2015 – LTE Access Class 14 for National Security and Emergency Preparedness (NS/EP) Communications • 3GPP Release 12 LTE and other standards used by a majority of wireless carriers in the United States. • Future standards as established by 3GPP and coordinated by FirstNet

A.1.5. SECURITY DOMAIN

The Security Domain encompasses the network, facility, and personnel security associated with the implementation of NG911 services. Specifically, this domain focuses on the policies, systems, and applications required to develop the access, network, and information security appropriate for each stage of the NG911 Maturity Model. Security is designed into the NG911 systems and most of the standards reflect this security by design. NENA standards require the use of Hypertext Transfer Protocol Secure (HTTPS) and TLS protocols between systems within an ESInet, and require authentication and authorization for access to systems and data.

Today, IPSRs, NGCS, and their security components are found in local, regional, and state pockets of deployment across the country, hence proving technical feasibility. The implementation of these systems is enabled by solution providers that have spent thousands of hours designing, developing, and testing their systems.

The ESInet and NGCS are secured through multiple components and system configurations. These components include firewalls, SBCs, IDSs, IPSs, and ICAM systems. These systems operate 24 x 7 x 365 and are managed by a SOC. In some cases, an NG911 service provider may consolidate these functions with its NOC. The NOC/SOC provides constant monitoring of the ESInet and NGCS, looking for anomalies and alarms. As incidents arise, the NOC/SOC is required to have SOPs in place for notifying customers and the FCC NORS.

The NENA i3 standard implements most of its network and information security controls by passing all NG911 traffic through the BCF. Access to the NG911 systems and applications is mainly controlled by operating system-level credentialing that replicates hierarchically across interconnecting domains, and which enables authorized users to operate at any location. Activities related to this domain are illustrated in the matrix found in Figure A-5 below.

Figure A-5: NG911 Security Domain Matrix

A.1.5.1.   Border Control Function (BCF)

The BCF provides perimeter security through its firewall, and VoIP call processing through its SBC. All PSAPs that have an externally accessible IP network today already have one or more firewalls, at all levels of the maturity model. Because it is highly desirable that the NG911 connection has its own dedicated firewall to assure homogenous implementation of routing and security rules on the ESInet, the cost model must include additional units for all PSAP and core interconnection points starting at the Transitional stage.

The SBC is necessary to process IP 911 calls and to anchor (i.e., temporarily store) the solicited and unsolicited 911 call multimedia content until it is delivered to the appropriate answering position or to another ESInet. The SBC also provides IP packet address conversion, data encryption/decryption, call bridging, quality-of-service (QoS) processing, call-detail recording, and performance measurements. IDSs and IPSs provide additional security in identifying and isolating penetrations of the network perimeter.

- BCF Available and Functioning – The BCF is installed, configured, and tested. The BCF manages all voice and data traffic entering and exiting the network. The BCF is in place beginning in the Transitional stage and continues throughout the End State stage.

Functional & Technical Requirements	Specifications/Standards
BCF detects intrusion or harmful data	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • NENA 08-506 – NENA Emergency Services IP Network Design for NG9-1-1 (NID) (including subsequent versions) • ATIS-0500019.2010 (R2015) – Request for Assistance Interface (RFAI) Specification • NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)
BCF reacts and prevents intrusion or harmful data from entering the system	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • NENA 08-506 – NENA Emergency Services IP Network Design for NG9-1-1 (NID) (including subsequent versions) • ATIS-0500019.2010 (R2015) – Request for Assistance Interface (RFAI) Specification • NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)
BCF receives data from the OSE	• 3GPP 23.167 – IP Multimedia Subsystem (IMS) emergency sessions • ATIS-PP-0500002.2008 (R2013) – Emergency Services Messaging Interface (ESMI)
BCF processes data, to include multimedia, without impact to the data	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision)

A.1.5.2.   Facility and Personnel Security

From an NG911 perspective, there is physical security—which is necessary to protect the NG911 system physical infrastructure—and cybersecurity, which requires policies, systems, and software to protect the integrity of the network and the confidential information it carries. Although it is possible to improve a PSAP's physical security to protect against acts of terror, such security generally is well implemented in legacy PSAPs.

Even in the most optimistic view, physical security will not prevent local, regional, or state NG911 computing or networking components from being compromised, intentionally or accidentally. The NG911 network only can be secured by implementing strong external and internal access controls supported by contemporary security policies that consider the new realities of cybersecurity.

One of the most important requirements for NG911 is that each system user be uniquely identifiable, and that their associated credentials must define their access rights for applications available from the network at that location. Furthermore, access to critical systems like NG911 must use dual-factor authentication, which provides greater assurance that the user is who they say they are, most especially when the system is accessed outside secured facilities, as in the case of mobile devices.

- Individual System Log-in – The individual user has a unique or shared username and password for accessing each 911 application, system, or auxiliary platform. Individual log-in is in place in the Legacy stage.

Functional & Technical Requirements	Specifications/Standards
NG911 components located in secure facilities to protect from malicious actions	- NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) - National Institute of Standards and Technology (NIST) – Framework for Improving Critical Infrastructure Cybersecurity - Criminal Justice Information Services (CJIS) Security Policy
Each person using system has a shared or unique log-in per system	- NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) - NIST – Framework for Improving Critical Infrastructure Cybersecurity

Functional & Technical Requirements	Specifications/Standards
Each person using system has a shared or unique log-in per system (continued)	• Criminal Justice Information Services (CJIS) Security Policy

- <u>Local, Regional, Statewide Single Log-in</u> – Each individual user has a unique username and password. This combination provides a single-factor log-in to all authorized 911 applications, systems, and auxiliary platforms, while mobile users would be required to use dual-factor authentication. Single-factor log-in begins in the Foundational stage and continues into the Intermediate stage.

Functional & Technical Requirements	Specifications/Standards
NG911 components located in secure facilities to protect from malicious actions	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • Criminal Justice Information Services (CJIS) Security Policy
Each person using the NG911 system has a unique shared log-in for local, regional, and state systems	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • Criminal Justice Information Services (CJIS) Security Policy
Identity management and user roles are in place regionally or statewide	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • Criminal Justice Information Services (CJIS) Security Policy • ISO/IEC[51] 24760-1 – Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts

---

[51] International Organization for Standardization/International Electrotechnical Commission

Functional & Technical Requirements	Specifications/Standards
Identity management and user roles are in place regionally or statewide (continued)	• ISO/IEC 24760-2 – Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements • ISO/IEC 24760-3 – Information technology – Security techniques – A framework for identity management – Part 3: Practice • ISO/IEC 29115 – Information technology – Security techniques – Entity authentication assurance framework • ISO/IEC 29146 – Information technology – Security techniques – A framework for access management • ISO/IEC WD 29003 – Information technology – Security techniques – Identity proofing

- Trustmark Access – Access is advanced to a trustmark framework enabling a scalable, agile environment for managing trusted access to all applicable 911 applications, systems, and auxiliary platforms. User credentials are replicated hierarchically so NG911 systems and applications can be accessed anywhere authorized. Dual-factor authentication is mandatory across the system. Trustmark access is in place in the End State stage.

Functional & Technical Requirements	Specifications/Standards
Identity management and user roles are in place nationally	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • Criminal Justice Information Services (CJIS) Security Policy

Functional & Technical Requirements	Specifications/Standards
Identity management and user roles are in place nationally (continued)	• ISO/IEC 24760-1 – Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts • ISO/IEC 24760-2 – Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements • ISO/IEC 24760-3 – Information technology – Security techniques – A framework for identity management – Part 3: Practice • ISO/IEC 29115 – Information technology – Security techniques – Entity authentication assurance framework • ISO/IEC 29146 – Information technology – Security techniques – A framework for access management • ISO/IEC WD 29003 – Information technology – Security techniques – Identity proofing
Information-sharing environment, trustmark framework is in place nationally	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • Criminal Justice Information Services (CJIS) Security Policy • Trustmark Framework Technical Specification

A.1.5.3.   Network and Security Monitoring

Network security is not an event, but rather a continuous process. Monitoring for security infractions and network integrity, combined with appropriate incident response, protects NG911 operations. NG911 is currently and will continue to be implemented within existing local, regional,

and state network infrastructures that have various levels of security rules and enforcement capabilities. Furthermore, many smaller PSAPs have very little exposure to security issues and will need assistance preparing for NG911 system security requirements. To assure the integrity of the national NG911 system, the National 911 Program will need to educate local authorities and PSAP managers about the new security policies and audit their readiness.

- <u>Monitoring, Incident Management and Response</u> – Network and security monitoring is operational with a defined incident management process in place. Coordinated response is practiced and executed when network problems and security infractions arise. Continuous improvement processes are in place to ensure that all incidents are met with comprehensive and effective issue mitigation techniques.

  A hierarchical design for security and network monitoring and management, as well as incident response and resolution, is the preferred methodology for implementation on a national scale. Local and regional NOCs and/or SOCs) would collect monitoring data at the local and regional level and pass it up to the state level. States would collect the regional data and pass it up to the national level. In some cases, there only may be a state-level NOC/SOC, or a NOC/SOC that monitors and manages a small group of states.

  At the national level, there may be three or four physical NOCs/SOCs for redundancy and resiliency, all with overarching access to the same data, and the view of attacks or outages provided by that overarching view.[52]

  Network monitoring, incident management, and response are implemented in the Foundational stage and continue throughout the End State stage.

Functional & Technical Requirements	Specifications/Standards
Provide network monitoring processes	- NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) - NIST – Framework for Improving Critical Infrastructure Cybersecurity - ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

---

[52] Section 6 of the TFOPA Working Group 1 report presents a conceptual design called Emergency Communications Cybersecurity Center (EC3) structured in this manner.

Functional & Technical Requirements	Specifications/Standards
Provide network monitoring processes (continued)	• ISO/IEC DIS 27004 – Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation • ISO/IEC 20000-1:2011 – Information technology – Service management – Part 1 – Service management system requirements
Develop and implement a comprehensive incident management and response plan	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements • ISO/IEC 20000-1:2011 – Information technology – Service Management – Part 1 – Service management system requirements
Manage and update the comprehensive incident management and response plan using data analytics, experience, and testing	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements • ISO/IEC 20000-1:2011 – Information technology – Service management – Part 1 – Service management system requirements

- Emerging Communications Cybersecurity Centers (EC3) – Network and security monitoring and response is operational with a defined incident management process in place. "The intent of the logical architecture recommendation is to create a centralized function, and location, for securing Next Generation (NG) networks and systems. By centralizing certain features, including cybersecurity in general, and intrusion detection and prevention services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place or at a minimum readily available for deployment and use."[53]

  The EC3 would be able to monitor networks and systems and react quickly to issues. They also would require a method to share and distribute information as needed to ensure that a coordinated response is practiced and executed when network problems and security infractions arise. Continuous improvement processes are in place to ensure that all incidents are met with comprehensive and effective issue-mitigation techniques. In some cases, there only may be a state-level NOC/SOC, or a NOC/SOC that monitors and manages a small group of states.

  At the national level, there may be three or four physical NOCs/SOCs for redundancy and resiliency, all with overarching access to the same data, and the view of attacks or outages provided by that overarching view.[54]

  Full EC3 functions are implemented in the Intermediate stage and continue throughout the End State stage.

Functional & Technical Requirements	Specifications/Standards
Provide network monitoring processes	- NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) - NIST – Framework for Improving Critical Infrastructure Cybersecurity - ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

---

[53] Task Force on Optimal PSAP Architecture, *Cybersecurity: Optimal Approach for PSAPs Supplementary Report*, (December 2, 2016), Working Group 1.

[54] Section 6 of the TFOPA Working Group 1 report presents a conceptual design called Emergency Communications Cybersecurity Center (EC3) structured in this manner.

Functional & Technical Requirements	Specifications/Standards
Provide network monitoring processes (continued)	• ISO/IEC DIS 27004 – Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation • ISO/IEC 20000-1:2011 – Information technology – Service management – Part 1 – Service management system requirements
Develop and implement a comprehensive incident management and response plan	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements • ISO/IEC 20000-1:2011 – Information technology – Service management – Part 1 – Service management system requirements
Manage and update the comprehensive incident management and response plan using data analytics, experience, and testing	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements • ISO/IEC 20000-1:2011 – Information technology – Service management – Part 1 – Service management system requirements

A.1.6. OPERATIONS/PERFORMANCE DOMAIN

The Operations/Performance Domain describes the policies, procedures, and programs that are needed to effectively operate NG911 systems. Activities related to this domain are depicted in the matrix found in Figure A-6 below.

Figure A-6: NG911 Operations/Performance Domain Matrix

A.1.6.1.   PSAP Training

Per the National 9-1-1 Assessment Guidelines, "Training should exist and be the same for all staff who perform telecommunicator duties."[55] In the Legacy stage today, the Association of Public-Safety Communications Officials (APCO) and the National Fire Protection Association (NFPA) have training standards for telecommunicators. Several agencies jointly published the Recommended Minimum Training Guidelines for Telecommunicators.[56] Some states have rules in place, or are in the process of adopting rules, to mandate state-level training standards. These state and national training standards will need to be updated as NG911 services, such as text, images, and video, are introduced.

- Develop, Implement, and Update PSAP Training – State, tribal, regional, or local 911 authorities will develop or adopt training standards for new types of information being presented to the PSAP. Training will be implemented at the state, regional, or local level in the Foundational stage, and continue to be monitored and updated on an ongoing basis through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Develop training standards for the telecommunicator	- APCO ANS 3.103.2.2015 – Minimum Training Standards for Public Safety Telecommunicators - Recommended Minimum Training Guidelines - APCO ANS 1.113.1-201x – Public Safety Communications Call Handling Process - APCO ANS 1.115.1-201x – Core Competencies, Operational Factors, and Training for Next Generation Technologies in Public Safety Communications - NFPA® 1061 – Professional Qualifications for Public Safety Telecommunications Personnel

---

[55] "Draft Report for National 9-1-1 Assessment Guidelines," 911 Resource Center, June 2012, https://resourcecenter.911.gov/911Guidelines/RPT053012_National_911_Assessment_Guidelines_Report_FINAL.pdf, section 5.6.

[56] "Recommended 911 Minimum Training for Telecommunicators," National 911 Program, https://www.911.gov/trainingguidelines.html.

Functional & Technical Requirements	Specifications/Standards
Develop training standards for the communications training officer	• APCO ANS 3.101.2-2013 – Core Competencies and Minimum Training Standards for Public Safety Communications Training Officer (CTO) • NFPA® 1061 – Professional Qualifications for Public Safety Telecommunications Personnel
Develop training standards for the public safety communications supervisor	• APCO ANS 3.102.1-2012 – Core Competencies and Minimum Training Standards for Public Safety Communications Supervisor • NFPA® 1061 – Professional Qualifications for Public Safety Telecommunications Personnel
Develop standards for next generation technologies in public safety communications	• APCO 1.115.1-201x – Core Competencies, Operational Factors, and Training for Next Generation Technologies in Public Safety Communications

A.1.6.2. Operational Procedures

Most SOPs are managed at the local PSAP level in the Legacy stage, with some state or regional entities regulating a minimum level of service delivery and/or performance standards.

Migrating to NG911 will give PSAPs the ability to natively handle SIP voice, text, multimedia, machine-to-machine, and other IP network-enabled call types. The any-to-any nature of IP networks also enhances the disaster-recovery options available to PSAPs. Implementing call-handling systems in a hosted model (e.g., colocated in data centers with the NGCS) enables PSAPs to deploy resources anywhere they have access to a secure broadband connection. Using a specially configured and secured laptop, personnel can log into the hosted call-handling system and take calls as if they were in their normal PSAP.

The implementation of the NG911 environment and IP-based networks enables native integration of new devices and services into the NG911 system. Examples include, but are not limited to, alarms, sensors, and other IP-based devices and services that may be developed in the future. The move to NG911 is the first step in getting supplemental data to emergency responders via FirstNet.

Operating agreements will be required between 911 authorities and service providers. These agreements will need to cover subjects such as SLAs, incident management, problem management, change management, and network and system monitoring. Vendors offer many levels of monitoring, so the desired level must be clearly stated in requests for proposals (RFPs) and contracts.

- <u>Develop, Implement, and Update Operational Procedures</u> – The state or region may develop or update procedures specific to NG911 to include: service delivery, performance, interface standards for data exchange/sharing, call processing, security, redundancy and reliability, and interdependencies between systems. Operational procedures are implemented in the Foundational stage and continue to be monitored and updated on an ongoing basis through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Develop or update procedures for data exchange	• APCO ANS 1.111.1-2013 – Public Safety Communications Common Disposition Codes for Data Exchange • APCO ANS 1.116.1-2015 – Public Safety Communications Common Status Codes for Data Exchange • APCO ANS 2.103.1-2012 – Public Safety Communications Common Incident Types for Data Exchange • NENA 71-501 – Information Document for Synchronizing Geographic Information System Databases with MSAG & ALI
Develop or update procedures specific to NG911 call-processing protocols	• NENA-INF-007.1-2013 – NENA Information Document for Handling Text-to-9-1-1 in the PSAP • NENA-INF-011.1-2014 – NG9-1-1 Policy Routing Rules Operations Guide
Develop procedure for the use of social media in public safety communications	• APCO ANS 1.112.1-2014 – Best Practices for The Use of Social Media in Public Safety Communications

Functional & Technical Requirements	Specifications/Standards
Develop or update procedures for performance and service delivery	• NFPA® 1221 – Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems
Develop operational procedures for PSAP preparedness, survivability, and sustainability amidst a wide range of natural and manmade events	• APCO/NENA ANS 1.102.2-2010 – Public Safety Answering Point (PSAP) Service Capability Criteria Rating Scale

A.1.6.3.   *Managed Services*

NGCS may be managed and maintained by the 911 authority, or procured in a managed services contractual arrangement that would include the service offering. Some models also enable a third-party managed-services provider to ensure vendor compliance with SLAs, and to have an additional level of review on the system, allowing for the 911 authority to focus on 911 operations.

- Develop, Implement, and Maintain Managed Services – Managed services may be deployed in conjunction with an ESInet or NGCS NOC. All NG911 components have a robust managed service provided by the 911 authority, its NGCS/ESInet solution provider, and/or a third party. 911 authorities having complex needs may have managed services provided by two or three potential providers for comprehensive oversight of system performance. Managed services are implemented in the Foundational stage and continue to be monitored and maintained on an ongoing basis through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Provide technical support 24 x 7 x 365	• ITIL Service Operation • ITIL Service Transition • SLAs • FCC rules and best practices
Provide a service portal for opening trouble tickets and checking status of existing tickets	• ITIL Service Operation • ITIL Service Transition
Provide documented change- and configuration-management procedures	• ITIL Service Operation • ITIL Service Transition

Functional & Technical Requirements	Specifications/Standards
Provide preventive maintenance	- ITIL Service Operation - ITIL Service Transition - Equipment vendor preventive maintenance recommendations
Cooperatively work with all NG911 system providers	- SLAs - FCC rules and best practices

A.1.6.4. *Service Level Agreements (SLAs)*

NENA recommends that prior to transitioning to NG911, 911 authorities determine the methodology to be used to ensure that network and system operation and reliability meet acceptable and adopted standards.[57] Solutions should provide the capability to monitor, record, and analyze system performance data against predefined metrics (e.g., establish system norms and flag exceptions).

SLAs cover the quality of the network in terms of latency, jitter, packet loss, and other measures; define incident response and escalation parameters; and set forth penalties for noncompliance. Incident response usually is based on the ITIL scale of Severity 1–4, with Severity 1 being the highest and thus having the shortest response time.

- Develop, Implement, and Maintain SLAs – The state or 911 authority determines and implements, through contract negotiations, the appropriate service levels. SLAs are implemented in the Foundational stage and continue to be monitored and maintained on an ongoing basis through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Define expected service level by system, component, and/or groups of systems	- FCC rules and best practices - NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) - NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)
Define reporting requirements	FCC rules and best practices

---

[57] "NG9-1-1 Planning Guidelines," National Emergency Number Association, January 8, 2014, https://www.nena.org/?page=ng911planning.

Functional & Technical Requirements	Specifications/Standards
Define implications for not meeting expected levels	• FCC rules and best practices
Define process for changes, updates, and maintenance of the agreements	• Local procurement rules

A.1.6.5. Contingency Plans

Contingency planning, often referred to as a continuity of operations plan (COOP), occurs at all levels of the hierarchy, from individual PSAPs to regions to states/territories to the national level. Neighboring PSAPs may come together to review each other's operations, staffing, location, etc. NENA publishes an informational document on contingency and disaster planning to assist 911 entities in developing, implementing, and testing their own plans.

- Develop, Implement, and Update Contingency Plans – The state or 911 authority develops and implements plans. Contingency plans are living documents and, as such, require regular reviews and updates. Contingency plans are developed in the Foundational stage, and a process of plan, review, update, test, and repeat should occur on an ongoing basis through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Develop a COOP	• Report for National 9-1-1 Assessment Guidelines • National Emergency Communications Plan • NFPA® 1221 – Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems • Continuity of Operations (COOP) Multi-Year Strategy and Program Management Plan Template Guide
Establish a process for reviews and updates to the plan	• Report for National 9-1-1 Assessment Guidelines • National Emergency Communications Plan

Functional & Technical Requirements	Specifications/Standards
Identify current level of PSAP service capability	• APCO/NENA ANS 1.102.2-2010 – Public Safety Answering Point (PSAP) Service Capability Criteria Rating Scale

A.1.6.6. Data QA and Analysis

NENA publishes recommended data requirements and data QA standards for 911 authorities to adopt. Data quality is monitored and maintained at the local level, and pushed up to successively higher levels in the hierarchy (regional, state, national, and international). Validation checks are performed at each level to ensure that the data is transferred cleanly and is properly formatted for that level.

- Develop, Implement, and Update Data QA – The state or 911 authority will develop or adopt standards for data quality, and develop policies and procedures to manage the data.

Functional & Technical Requirements	Specifications/Standards
Develop data requirements and standards	• NENA 02-010 – Standard Data Formats for 9-1-1 Data Exchange & GIS Mapping • NENA 02-014 – GIS Data Collection and Maintenance Standards • NENA-02-010 – Standard Data Formats For 9-1-1 Data Exchange & GIS Mapping[58]
Develop a quality assurance process	• NENA 02-010 – Standard Data Formats for 9-1-1 Data Exchange & GIS Mapping • NENA 02-014 – GIS Data Collection and Maintenance Standards
Maintain and update data standards and processes	• Local procurement rules • Governance plans

---

[58] NENA-STA-006.1-201X – NG9-1-1 GIS Data Model – will replace this standard when complete.

A.1.6.7.   System Testing

Each system, procedure, and data element is important to NG911 systems. A comprehensive technical system testing program should be in place, including data auditing, system metric testing, and security testing.

- Develop, Implement, and Maintain System Testing – The state or 911 authority develops, implements, and maintains comprehensive testing of all systems, data, and procedures to ensure compliance and effectiveness of the NG911 systems. System testing will begin in the Foundational stage and continue through the End State stage.

Functional & Technical Requirements	Specifications/Standards
Define testing measures and methods	• NENA-STA-010.2-2016 – Detailed Functional and Interface Standards for the NENA i3 Solution (under revision) • NENA 08-506 – NENA Emergency Services IP Network Design for NG9-1-1 (NID) (including subsequent versions) • NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST Framework for Improving Critical Infrastructure Cybersecurity • SLAs
Develop and implement testing plan	• Local policies and procedures • NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST Framework for Improving Critical Infrastructure Cybersecurity • Principles of ethical hacking
Maintain and update testing plan regularly	• Local policies and procedures • NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST Framework for Improving Critical Infrastructure Cybersecurity

A.1.6.8. Cybersecurity Program

The development and maintenance of a cybersecurity program is required as 911 authorities begin to operate in an IP-based environment, regardless of whether the operations encompass CAD, radio, or NG911 call delivery and call handling. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[59] provides a structure of functions and categories that may assist 911 authorities in developing a cybersecurity program that captures the methodologies and outcomes that are customized and appropriate for the 911 authority's operations. Cybersecurity programs should provide documented breach prevention, mitigation, redundancy, reporting, and recovery procedures.

- Multiple Diverse System Cybersecurity Programs – IP systems are deployed in silos with limited security services from IP network providers. Cybersecurity processes and awareness are isolated and limited in deployment. Diverse cybersecurity programs will begin to appear in the Foundational stage and continue through the Transitional stage.

Functional & Technical Requirements	Specifications/Standards
Each system or provider develops a cybersecurity program	- Local policies and procedures - NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) - NIST – Framework for Improving Critical Infrastructure Cybersecurity

- Coordinated Cross-system Cybersecurity Program – The cybersecurity program across all systems and vendors is ingrained in operations, with maintenance processes established to enable the program to evolve as operations, threats, and vulnerabilities change. Coordinated cross-system cybersecurity programs will begin to appear in the Intermediate stage and continue through the End State stage.

---

[59] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, (February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

Functional & Technical Requirements	Specifications/Standards
Each separate cybersecurity plan adheres to a set of common principles and goals	• Local policies and procedures • NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
Each separate entity shares a common cybersecurity program	• Local policies and procedures • NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
Information on immediate and potential threats, risks, and attacks are shared across all systems interconnected to NG911 systems	• NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) • NIST – Framework for Improving Critical Infrastructure Cybersecurity • ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements • Object Management Group (OMG) – Unified Modeling Language™ (UML®) Operational Threat & Risk Model (under development)

- National-Level Cybersecurity Monitoring and Response – There is a national-level, coordinated, cross-system cybersecurity program to respond to incidents. This national Computer Emergency Readiness Team (CERT), EC3, or intrusion detection and prevention services (IDPS) will exist in the End State stage.

Functional & Technical Requirements	Specifications/Standards
Each separate cybersecurity plan adheres to a set of common principles and goals	- Local policies and procedures - NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) - NIST – Framework for Improving Critical Infrastructure Cybersecurity - ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
Each separate entity shares a common cybersecurity program	- Local policies and procedures - NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) - NIST – Framework for Improving Critical Infrastructure Cybersecurity - ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
Information on immediate and potential threats, risks, and attacks are shared across all systems interconnected to NG911 systems	- NENA 75-001 – NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) - NIST – Framework for Improving Critical Infrastructure Cybersecurity - ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements - Object Management Group (OMG) – Unified Modeling Language™ (UML®) Operational Threat & Risk Model (under development)

A.2. Architecture

NG911 is an enterprise solution that will result in a nationwide system of systems that must share a common approach and be interoperable. The NG911 architecture for the cost study depicts a high-level view of a complete NG911 continuum, including legacy, transitional, and end-state components (see Figure A-7 below). Transitional elements such as the legacy gateways and IPSR will be decommissioned when the end state is reached, or as legacy originating and terminating systems are decommissioned.
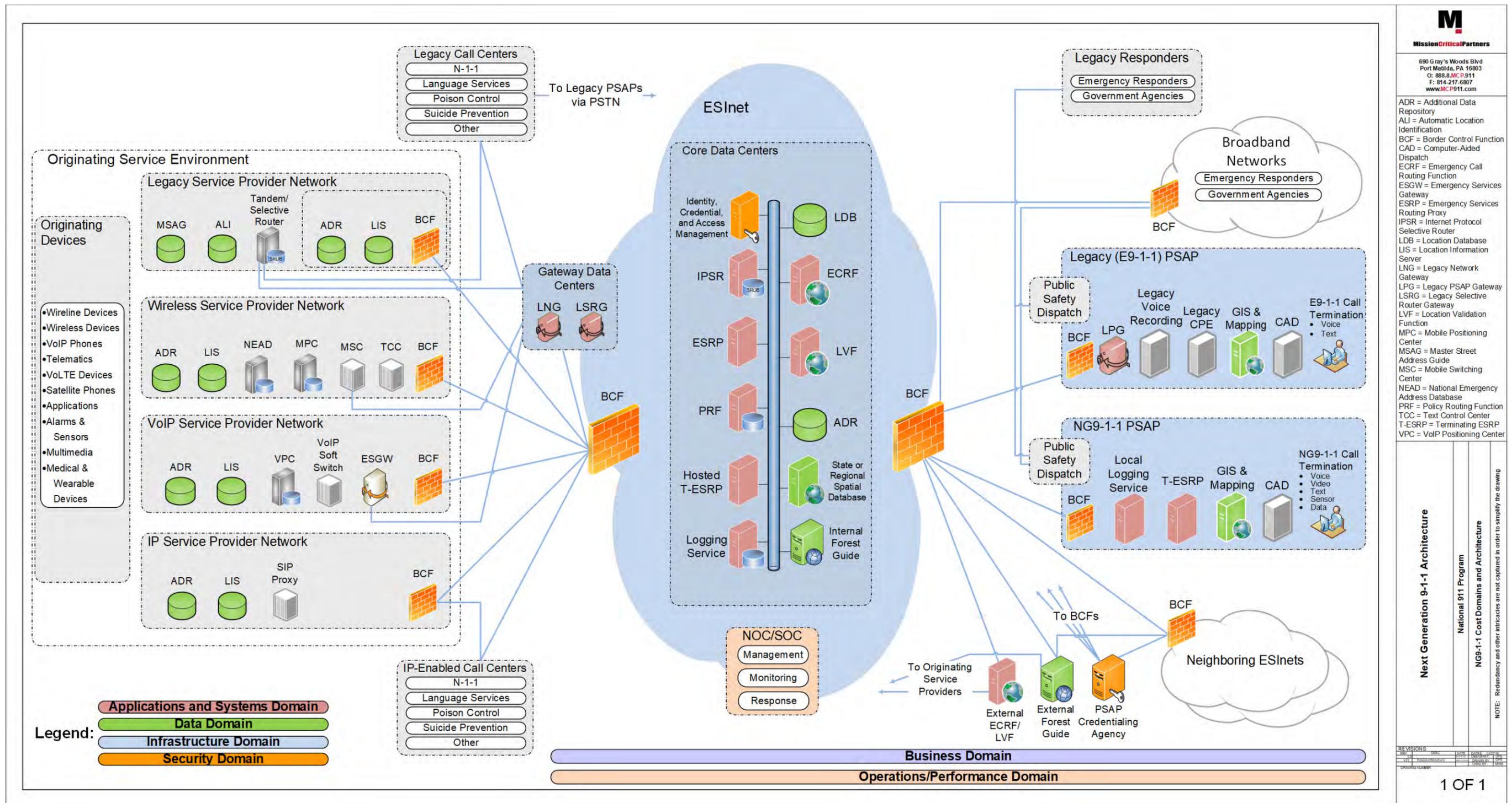
Figure A-7: NG911 Cost Study Architecture Diagram

All components of the NG911 cost study architecture are included in the NG911 Maturity Model; however, the model adds the stages of deployment. The NG911 Maturity Model was the basis of the cost analysis to determine the cost elements and timing of deployments throughout the ten-year lifecycle. The NG911 Cost Study architecture is described below.

A.2.1. ORIGINATING SERVICE ENVIRONMENT

The OSE consists of the devices and systems necessary to establish a call or request for service. For the purposes of this document, the term "call" refers to any request regardless of the form it takes or the technology employed to deliver information to a PSAP. This includes wireline, wireless, and VoIP voice calls; teletypewriter/telecommunications device for the deaf (TTY/TDD) calls; alarms; telematics; text messaging; and any other technology that may be used to report an emergency.

Originating devices may take many forms: telephones, private branch exchanges (PBXs), unified communications (UC) systems, smartphones, tablets, personal computers (PCs), alarm systems, vehicles, healthcare devices, and machines.

The legacy service provider network has an IP connection to allow access from the ESInet to a provider-based ADR and LIS. The MSAG and ALI services still are accessed via TDM connections.

Call centers, both TDM-based and IP-based, are shown outside the OSE with connections to both the OSE and the ESInet/PSAP environment. These centers will seldom truly originate a call, but will frequently be a party to a 911 call.

A.2.2. NG911 CORE AND ESINET

During the Foundational and Transitional stages, TDM traffic will be delivered from the legacy providers to gateway data centers for conversion to SIP by the LNGs. When the Intermediate stage is reached, the incoming gateways will be decommissioned. The ESInet provides the underlying transport for the services and systems that will handle the emergency calls. BCFs provide security for the ESInet and protection of incoming and outgoing IP traffic. The NOC and SOC, which may be combined or separate facilities, monitor the health and security of the network, provide problem- and change-management functions, report as required on all aspects of the status and health of the network and its systems and services, and coordinate response to system or network issues.

The services within the core data centers are collectively referred to as NGCS. These are the services required to process a call from its entry into the ESInet to its delivery to the PSAP

workstation. The IPSR is a transitional element providing SIP-based routing functions using legacy MSAG and ALI records. This element is decommissioned at the end of the Transitional stage. Some PSAPs may migrate directly to the Intermediate stage, bypassing the use of an IPSR.

The ESRP also provides call-routing functionality, but relies on queries to geospatial data in the ECRF. There may be multiple ESRPs involved in routing a call to the proper PSAP. Call-handling systems that are considered i3-capable often are referred to as Terminating ESRPs (T-ESRPs) because they use the same methodology to route the call to a specific telecommunicator for call handling. There also may be a hosted instance of a call-handling system, where the back-office systems are in the core data centers, and only the workstations are at the PSAP.

The PRF is a database of special routing rules that typically reside in the ESRP, which may override the routing instructions returned from the ECRF. Special rules for time-of-day, special events, natural disasters, or PSAP evacuations are configured and stored in the PRF. At the appropriate time, a rule may be invoked to redirect calls from one PSAP to another PSAP capable of handling them.

The ECRF queries location data based on the SIP header information passed to it from the ESRP. It then returns routing information that enables the ESRP to properly route the call. The LVF is a mirror image of the data that resides in the ECRF, and is queried by the LIS to validate civic location information prior to a call being placed.

The event logger maintains transaction records from every system or service that handles a given call, along with the media streams associated with the call. Locating the event logger with the NGCS allows for pre-answer recording of the media streams. This does not preclude any PSAP from maintaining a local event logger. Such a device may be utilized to log local event data in case the PSAP is severed from the ESInet and is working in a local survivability mode where it is only receiving calls on administrative lines separate from the ESInet connection.

The LDB is a hybrid database that combines the functionality and interfaces from legacy ALI databases with the NG911 functionality and interfaces of the LIS and ADR. As a transitional element, it enables an i3 call flow in an environment where carriers continue to submit legacy SOIs and do not yet provide their own LIS and ADR services.

The ADR contains additional information about a variety of subjects related to a given call, caller, or location. This may include, but is not limited to, subscriber information, medical information, building floor plans, and emergency contact information.

A local copy of state or regional GIS data also may be maintained within the NGCS, along with local instances of security, credential, and access-management data. The state or regional GIS data

will use a spatial interface to provide data updates to the elements using GIS data, such as the LVF, ECRF, call-handling system, and CAD mapping application.

A.2.3. PSAPS

The legacy PSAP has CPE that is not capable of handling SIP or i3 calls. An LPG connects the PSAP to the ESInet, allowing SIP calls to be routed to the PSAP. The LPG is protected by a BCF instance. The legacy PSAP may maintain TDM connections to its service providers until such time as the CPE is upgraded to an i3-capable call-handling system. The legacy PSAP will have connectivity to legacy responders for dispatching resources to a call incident.

The NG911 PSAP is an all-IP, i3-capable PSAP. This PSAP is depicted with the call-handling system (T-ESRP) residing locally at the PSAP. The NG911 PSAP may have connectivity to both legacy-enabled responders and IP-enabled responders served by FirstNet.

A.2.4. OTHER SUPPORTING SYSTEMS

The National Emergency Address Database (NEAD) is a developing solution that will enable mobile devices to provide a dispatchable location; it is especially designed to solve issues with the challenges associated with locating wireless callers indoors and in multitenant buildings. The NEAD will house detailed location information for access points and beacons, including street address, floor, suite, apartment, or other location information.

The Forest Guide is a repository of location and routing information that may be queried to determine suggested call routing for a call that cannot be routed by the local or regional routing data. The PSAP Credentialing Agency provides and authenticates security credentials for the various components of the NGCS and PSAPs.

This page is intentionally left blank.

APPENDIX B – NG911 MATURITY MODEL

B.1. BUSINESS DOMAIN

More than half of the nation, or 58 percent, has begun planning for Next Generation 911 (NG911) and about a fourth of the nation has a transition plan in place. In addition, slightly more than a fourth of the nation has completed a governance gap analysis, and about 6 percent of the nation has a governance plan in place that is being reviewed on a regular basis.

In addition, more than 38 percent of the nation has begun to procure an Internet Protocol (IP) network or NG911 services, and about 25 percent of the nation has implemented, or begun to implement, an IP network or NG911 services.

Table B-1: Business Domain National Progress

	Legacy	Foundational	Transitional	Intermediate	End State
Planning	42.0%	32.0%		26.0%	
Governance	67.2%	26.7%	0.2%	5.9%	
Policy	96.4%	2.6%	1.0%		
National Governance	100%				
Procurement	61.2%	22.4%	7.1%	9.3%	
Implementation	74.5%	14.6%	9.3%	1.6%	

B.2. DATA DOMAIN

About one-third of the nation is in the Transitional phase and has geocoded their addresses to a geographic information system (GIS)-ready format. This number is expected to increase slightly with further outreach and data gathering; however, this is one of the slower-moving areas of the NG911 transition. About 11 percent of the nation uses Location Databases (LDBs) rather than traditional automatic location identification (ALI) databases.

Table B-2: Data Domain National Progress

	Legacy	Foundational	Transitional	Intermediate	End State
Geographic Information System	67.3%		32.7%		
Location Data	88.9%			11.1%	
Additional Data	100%				
System Control and Management	100%				

B.3. APPLICATIONS AND SYSTEMS DOMAIN

Research found that only 13 percent of the nation is served by NG911-capable services. However, one positive note is that the migration of public safety answering points (PSAPs) to IP-capable call-handling equipment is well under way, with about 55 percent of the nation covered by IP-capable equipment at the PSAP. The delivery of location data via an Emergency Services IP network (ESInet) to the PSAP is at about 13 percent.

There is a large migration of legacy ALI circuits to IP circuits because of the reduction of support for legacy analog circuits by telephone providers. Almost 70 percent of the PSAPs have this technology, but the equipment at the PSAPs still receives legacy ALI data in most instances.

Table B-3: Applications and Systems Domain National Progress

	Legacy	Foundational	Transitional	Intermediate	End State
Call Routing	87.0%	10.0%		3.0%	
Call Handling Systems	45.0%			55.0%	
Location Validation	85.1%			14.9%	
Location Delivery	17.1%	69.7%	8.0%	5.2%	
Call Processing	100%				
Event Logging	100%				
Data Analytics	100%				
Forest Guide	100%				

B.4. INFRASTRUCTURE DOMAIN

Research found that only 22 percent of the nation is served by an ESInet, and 25 percent of the nation has data centers in place.

Table B-4: Infrastructure Domain National Progress

	Legacy	Foundational	Transitional	Intermediate	End State
Data Center	75.4%	24.6%			
Ingress Network	85.7%	9.2%		5.1%	
Egress Network	85.2%	7.2%		7.6%	
ESInet	78.4%	21.6%			
Network Operations Center (NOC)	80.8%	19.2%			
Non-voice Requests for Service	100%				
Network-to-Network Interface (NNI)	100%				
PSAP-to-Responder Network	100%				

B.5. SECURITY DOMAIN

Very limited data exists concerning the Security Domain, but the Federal Communications Commission (FCC) survey did ask if cybersecurity was being planned or underway in individual states. The survey revealed that most of the nation still is covered by legacy siloed and proprietary security measures; this does not mean there is no security, but that various systems are usually independent. Those 911 authorities that have deployed Next Generation Core Services (NGCS) from a vendor have security as part of that service, but may not be aware of the full level of that security.

Table B-5: Security Domain National Progress

	Legacy	Foundational	Transitional	Intermediate	End State
Border Control Function (BCF)	82.1%		17.9%		
Facility and Personnel Security	97.8%	2.2%			
Network and Security Monitoring	80.8%	19.2%			

B.6. OPERATIONS/PERFORMANCE DOMAIN

The Operations/Performance Domain also has limited information concerning it. This domain focuses on the operation of an NG911 system on an ongoing basis. With the NG911 migration still at an early stage, the actual needs of PSAPs and the changes from traditional 911 operations still are being developed. Activities such as the Interstate Playbook project of the National 911 Program are an example of the work that continues.

Table B-6: Operations/Performance Domain National Progress

	Legacy	Foundational	Transitional	Intermediate	End State
PSAP Training	99.6%	0.4%			
Operational Procedures	100%				
Managed Services	100%				
Service Level Agreements (SLAs)	100%				
Contingency Plans	91.7%	8.3%			
Data QA	100%				
System Training	100%				
Cybersecurity Program	92.9%	7.1%			

APPENDIX C – DETAILED NG911 ANALYSIS

In an emergency, the public expects the 911 system to function efficiently and effectively, anytime and anywhere, and for good reason. Since its implementation in the 1960s, the 911 system is credited with saving countless lives each year, and is a lifeline for people calling for help during emergencies.

However, despite its essential significance to the preservation of life and property, funding the 911 system poses an increasing challenge for the state and local governments charged with its operation. Some 911 authorities and public safety answering points (PSAPs) are finding that legacy funding mechanisms are inadequate to sustain current needs and clearly pose a challenge for future 911 operations. This challenge is being exacerbated by the need to transition old systems to Next Generation 911 (NG911) technology. NG911 will introduce numerous advanced capabilities, but it also will require a significant technology migration in order to reap its benefits. At the very least, significant challenges to funding both legacy 911 and the transition to NG911—when both networks need to be operational for some interim period of time—are a concern for many 9-1-1 authorities.

Congress, through its enactment of the Middle Class Tax Relief and Job Creation Act of 2012 (Pub.L. 112–96)—which also authorized the First Responder Network Authority (FirstNet) and the Nationwide Public Safety Broadband Network (NPSBN)—directed the Implementation Coordination Office (ICO)—in consultation with the National Highway Traffic Safety Administration (NHTSA), the Federal Communications Commission (FCC), and the Department of Homeland Security (DHS)—to develop a report that analyzes and determines detailed costs for implementing NG911 service nationwide.

By statute, "the purpose of the report is to serve as a resource for Congress as it considers creating a coordinated, long-term funding mechanism for the deployment and operation, accessibility, application development, equipment procurement, and training of personnel for Next Generation 911 services." To that end, this appendix provides the following:

- An assessment of the architectural characteristics, feasibility, and limitations of NG911 service delivery
- An analysis of the need for NG911 services by persons with disabilities

NG911 is an enterprise solution (multi-faceted approach to solving inefficiencies) that will result in a nationwide system of systems that must share a common approach and be interoperable. Consequently, the 911 community generally agrees that NG911 implementations must be standards-based, and for such implementations to be fully effective, they also must be standards-compliant. In instances where standards do not exist for elements within the NG911 Maturity Model—which was developed to measure the progress nationwide toward NG911 implementation

and is based on elements needed for NG911—industry informational documents and best practices were cited. The NG911 Maturity Model is used throughout the NG911 Cost Study Project.

The NG911 Maturity Model is based on the functional and operational elements that are needed for NG911 implementation. While some flexibility exists concerning the order in which some components may be deployed, the NG911 Maturity Model was developed at a high level to identify the costs associated with NG911. It is not a detailed engineering specification. The standards bodies will continue to develop the technical specifications needed to implement NG911.

The approach for this appendix consisted of applying the NG911 Maturity Model based on the functional and operational elements necessary for NG911, and identifying any gaps or potential issues.

C.1. ARCHITECTURAL CHARACTERISTICS, FEASIBILITY, AND LIMITATIONS OF NG911 ASSESSMENT

This assessment focuses on three main segments of the NG911 architecture: the originating service environment; the Next Generation Core Services (NGCS); and the PSAP and responders' environment. These segments, which may be viewed in the NG911 Cost Study Architectural Diagram found in Appendix A, are examined below.

C.1.1. ORIGINATING SERVICE ENVIRONMENT

C.1.1.1. *Architectural Characteristics*

The migration to NG911 will require service providers to make significant changes in the originating service environment (OSE). Service providers must migrate from the current Time Division Multiplexing (TDM) call-delivery environment to Session Initiation Protocol (SIP) delivery over Internet Protocol (IP) networks. Service providers are moving slowly from the legacy Public Switched Telephone Network (PSTN) Class 5 switches to IP-based softswitches using SIP to deliver calls. During the transition period from the legacy environment to NG911, the service providers will have to install legacy network gateways to translate the TDM circuits to SIP for delivery across an Emergency Services IP network (ESInet). Once the transition to the NG911 end state is complete, the gateway functionality will be decommissioned, though the physical devices may remain in service to perform other vital network functions.

One major change that NG911 brings concerns the delivery of the location information. This information currently is delivered via an automatic location identification (ALI) bid to a database after the call is answered by the PSAP. In the NG911 environment, the location information is delivered to the PSAP in the call's SIP message headers, although the location information still

can be updated by the call-taker during the call. The service providers will be required to develop and manage their own location information server (LIS) to provide the location information in the initial call delivery, and to provide updates throughout the call process.

As the PSTN migrates to an IP-based system, outside call centers such as poison control, language lines, N-1-1, and others will require upgrades to their systems and infrastructure in order to handle SIP calls. In the transition period, gateways may be required to connect these outside call centers to the PSAP network.

The implementation of the NG911 and IP-based networks enables native integration of new devices and services into the NG911 system. Examples include, but are not limited to, alarms, sensors, and other future IP-based devices and services.

C.1.1.2.   Feasibility

Service level agreements (SLAs) address the quality of the network in terms of latency, jitter, packet loss, and other measures; define incident response and escalation parameters; and set forth penalties for noncompliance. Incident response, usually is based on the well-established Information Technology Infrastructure Library (ITIL) Scale of Severity 1-4, with Severity 1 being the highest level and thus having the shortest required repair time.

Operating agreements will be required between 911 authorities and service providers. These agreements should cover subjects such as SLAs, incident management, problem management, change management, outage reporting requirements, and network and system monitoring. There are many levels of monitoring service offered by vendors, so the desired requirements must be stated clearly in requests for proposals (RFPs) and contracts.

Service providers are implementing IP Multimedia Subsystem (IMS) in their networks as a means of delivering multimedia traffic across many different device types. IMS makes use of many of the Internet Engineering Task Force (IETF) documents related to IP multimedia, including SIP. Because individual vendors interpret standards differently, SIP may not align properly between that which is implemented in IMS and that which is used in the National Emergency Number Association (NENA) i3 environment. Service providers may incur costs associated with transcoding SIP messaging exchanged between IMS and i3-compliant systems.

C.1.1.3.   Limitations

The timeline for service provider network migration from TDM to SIP delivery varies widely and will impact both cost and ubiquity in the networks. Even a given service provider may be moving at different paces within its own network. Many of the regional and local carriers already have

made the move to softswitches and voice over IP (VoIP), but are converting their 911 calls to TDM and passing the calls to the incumbent local exchange carrier (LEC) for aggregation.

Although SIP is defined in the IETF standards, each vendor has its own interpretation of the standards. What one vendor views as mandatory, another views as optional. Incompatibilities will exist between versions of SIP implemented both by the service providers and by the 911 authorities, causing a potential gap in the operational effectiveness of systems. Workarounds will have to be implemented to overcome these discrepancies in standards interpretations.

Another limitation within the OSE concerns the current process for acquiring location information for mobile callers. Current technologies used for identifying the location of wireless callers require a substantial amount of time to provide a routable Phase II location.

In November 2013, Verizon reported that only 65 percent of calls were able to obtain a Phase II fix within 13 seconds, and 99 percent of calls were able to obtain a Phase II fix within 25 seconds.[60] This and other data contributed to the FCC's update of the location accuracy rules in April 2015 to include a Time to First Fix (TTFF) of 30 seconds.[61] When every second counts, it is not reasonable to hold a call for 30 seconds to obtain a Phase II location in order to determine the appropriate route.

Because of these current limitations, wireless calls, which now make up 76 percent of 911 calls,[62] will not be able to benefit from NG911's enhanced ability to accurately route 911 callers to the best PSAP until wireless location technology improves.

NG911 provides the ability to route calls to the best PSAP based on the location of the caller at the time the call was made. Compared to today's legacy call-routing process, this will be a significant improvement, but until improvements are made to location-acquisition systems and processes, and NG911 is transitioned into the nation's PSAPs, this benefit will not be realized.

NEEDS:

Outside calls centers supporting PSAP operations should be engaged early in the planning process.

---

[60] Workshop On E911 Phase II Location, available at:
https://transition.fcc.gov/bureaus/pshs/911/Phase%202/Workshop_11_2013/VZW_E911_Location_Overview_Nov2013.pdf.
[61] Can be found at: https://www.federalregister.gov/articles/2015/03/04/2015-04424/wireless-e911-location-accuracy-requirements#h-7.
[62] Can be found at: http://www.911.gov/pdf/National-911-Program-2015-ProfileDatabaseProgressReport-021716.pdf.

Nationwide guidance to develop model operating agreements that address requirements for outside call center connectivity in the network are needed for 911 authorities and service providers.

Timelines and costs should be well understood between the 911 authority and the service provider(s).

Carriers should continue to improve the location-determination technologies and the delivery of a dispatchable location[63] to the PSAP with the call delivery.

C.1.2. CORE SERVICES

C.1.2.1. *Architectural Characteristics*

The NGCS are a collection of functional elements that each serve a role in routing a call to the proper PSAP. Each ESInet will have its own NGCS that will interoperate with adjacent NGCS to enable call and data transfer between PSAPs that are served by independent ESInets. Currently, the core services cannot operate independently without transitional components such as the OSE gateways previously discussed. Until the full end-state transition is complete, this will continue to be a gap requiring transitional components.

Transitional components enable PSAPs and originating service providers (OSPs) to migrate from the legacy environment to an NG911 environment without wholesale replacement of infrastructure. Deployment of an IP Selective Router (IPSR) is a transitional strategy that enables PSAPs to migrate to an ESInet while they develop their geographic information system (GIS) data, staff, and operational processes to support the i3 location-validation and geospatial call-routing functions. While an IPSR is not a component within the i3-compliant NGCS as it is a transitional element, its position is the same as NGCS in the call flow.

Alternatively, PSAPs may migrate directly to an ESInet with NGCS if they have the GIS data, staff and operational processes in place. PSAPs that elect this path will benefit immediately from geospatial call routing, validating caller locations based on the most current GIS data, and the implementation of policy routing rules, which allow for more-robust means to distribute call loads across a 911 authority's jurisdiction or region. PSAPs that migrate directly to an i3 NGCS-based solution eliminate the eventual transition from an IPSR to an i3 NGCS—which will be required for those that first deploy an IPSR—and thus avoid the costs related to a two-tiered transition.

---

[63] The FCC defines ''dispatchable location'' as the verified or corroborated street address of the calling party plus additional information such as floor, suite, apartment or similar information that may be needed to adequately identify the location of the calling party.

A major driver for implementation of NGCS is that the systems are software-based and the requests for assistance are delivered to it over an IP network. These two characteristics provide enormous flexibility for accommodating future technologies as the 911 call sources expand and new devices and services are introduced to the public. For example, the legacy 911 system today cannot accommodate the delivery of health data available from medical sensors. In contrast, an ESInet powered by NGCS would be able to support the delivery of this crucial data to telecommunicators and first responders. The flexible architecture of the NGCS enables it to accommodate future generations of sensors and services as they enter the marketplace.

The ESInet and NGCS are secured through multiple components and system configurations. These components include firewalls; session border controllers (SBC); intrusion detection systems (IDS); intrusion prevention systems (IPS); and identity, credentialing, and authentication management (ICAM) systems. These systems operate 24 x 7 x 365 and are managed by a security operations center (SOC). In some cases, an NG911 service provider may choose to consolidate these functions with its network operations center (NOC). The NOC/SOC provides constant monitoring of the ESInet and NGCS, looking for anomalies and alarms. As incidents arise, the NOC/SOC is required to have standard operating procedures (SOPs) in place for notifying customers and the FCC Network Operations Reporting System (NORS).

C.1.2.2. Feasibility

Today, IPSRs, NGCS, and their security components are found in local, regional and state pockets of deployment across the country, proving their technical feasibility. The implementation of these systems is enabled by solution providers that have spent human and technological resources designing, developing and testing their systems. ESInets and NGCS require sophisticated, complex software engineering that is integrated with VoIP network engineering. These NG911 service providers are required to enter into interconnection agreements with OSPs and legacy 911 service providers to be able to receive and transfer 911 calls.

911 authorities that choose to deploy a "*build, own and operate model*" also have to enter into these same agreements. States and regions must assess the extent of their desire for taking on the operational requirements and legal responsibilities for building, owning and operating their own ESInet with NGCS. In many cases, the depth and breadth of technical expertise required to support this model often will sway a 911 authority to look at the alternative services-based model. In these cases, a well-defined scope of work and strong SLAs provide 911 authorities with assurances regarding the level of service and extreme system availability required for 911 public safety services.

C.1.2.3.   Limitations

While IPSR solutions may provide a strategic advantage to PSAPs that have limited GIS data, they are restricted to legacy tabular-based routing rules that do not support advanced technologies such as sensor-based requests for assistance. Many 911 authorities face challenges in developing and maintaining their GIS data, which is a critical element to the proper function of NGCS. These challenges come in multiple forms. The development and maintenance of GIS data requires specialized expertise and dedicated resources to support these functions. For many jurisdictions, these positions are filled by one or two people, if anyone at all, or the duties are shared with other responsibilities that often have higher-priority requirements. In addition, local knowledge of the jurisdiction and region at large enables more precise data management. The combination of the critical role of these positions, the need for technical expertise and local knowledge, and limited staff makes it difficult to adequately develop and maintain GIS data. The demands of the position, the critical nature of the work, and the work load contributes to high turnover in these positions, and thus a threat to operations.

Another limitation of NGCS concerns the complexity and expense of deploying these systems. These limitations often drive small and rural 911 authorities to combine to create larger systems. NGCS are deployed most efficiently and effectively for regions with large populations, at a state level, or across a multistate region.[64] This limits 911 authorities in terms of procuring and deploying their own autonomous NGCS.

Transitional elements will be required while 911 authorities develop supporting GIS data, staff, and operational processes for the i3 location-validation and geospatial call-routing functions.

The NOC/SOC is required to have SOPs in place for notifying customers and the FCC NORS, and these SOPs are not yet developed.

Interconnection agreements with OSPs and legacy 911 service providers will be required to enable the receipt and transfer of 911 calls.

Examples of a well-defined scope of work (SOW) and strong SLAs to provide 911 authorities with assurances regarding the required level of service needs and system availability requirements do not exist.

NG911 GIS maintenance requirements require extensive technical expertise. The expertise required to manage the complexity of planning and deploying these systems, and the high cost of transition, presents a technical and funding gap.

---

[64] Task Force on Optimal PSAP Architecture, *Adopted Final Report,* (January 29, 2016), Federal Communications Commission, https://apps.fcc.gov/edocs_public/attachmatch/DA-16-179A2.pdf, page 148.

NEEDS:

Complete the development of supporting GIS data, staff, and operational processes for the i3 location-validation and geospatial call-routing functions.

National leadership is needed to develop model interconnection agreements between OSPs and legacy service providers, and SOW and SLA models for 911 authorities to follow.

Secure GIS expertise of the level necessary to support the critical nature of the 911 support systems.

Secure sustainable funding to address the challenges of transition and ongoing maintenance of NG911.

C.1.3. PSAPS AND RESPONDERS

C.1.3.1.   *Architectural Characteristics*

Migrating to NG911 will give PSAPs the ability to effectively handle SIP voice, text, multimedia, machine-to-machine, and other IP network-enabled call types. The any-to-any nature of IP networks also enhances the disaster recovery options available to PSAPs. Implementing call-handling systems in a hosted model (e.g., colocated in data centers with the NGCS) enables PSAPs to deploy resources anywhere they have access to a secure broadband connection. Using a specially configured and secured laptop, personnel can log into the hosted call-handling system and take calls from any client on the system as if they were in their normal PSAP facility.

The implementation of the NG911 environment and IP-based networks enables native integration of new devices and services into the NG911 system. Examples include, but are not limited to, alarms, sensors, and other IP-based devices and services that may be developed in the future. The move to NG911 is also the first step in getting supplemental data to emergency responders via responder networks such as the FirstNet NPSBN.

C.1.3.2.   *Feasibility*

Operating agreements will be required between 911 authorities and service providers. These agreements will have to cover subjects such as SLAs, incident management, problem management, change management, and network and system monitoring. There are many levels of monitoring offered by vendors, so the desired level must be clearly stated in RFPs and contracts.

SLAs cover the quality of the network in terms of latency, jitter, packet loss, and other measures; define incident response and escalation parameters; and set forth penalties for noncompliance. Incident response usually is based on the ITIL Scale of Severity 1-4, with Severity 1 being the highest and thus having the shortest response time.

NG911 requires advanced call-handling systems and, in some cases, will require the PSAP to upgrade its call-handling system to accept the new call types. PSAP logging and recording also will require change with the transition to an IP-based system. Ancillary systems also may require upgrades to be compatible with NG911 call-handling systems. Such ancillary systems may include but are not limited to, computer-aided dispatch (CAD) systems, management information systems (MIS), and records management systems (RMS).

C.1.3.3.   *Limitations*

Although broadband is considered to be widely deployed, there are areas in the country where it either is not deployed, or is deployed but with bandwidth limitations. The limitations may be due to distance, loop quality, or other factors.

PSAPs may experience issues with variations in implementation of the SIP standards much like the service providers in the OSE, though most of those issues should be addressed between the OSE and core services. As we have noted elsewhere in this appendix, although SIP is defined in the IETF standards, each vendor has its own interpretation of the standards. Incompatibilities will exist between versions of SIP implemented by the service providers, the NGCS, and the 911 authorities' call-handling equipment. Workarounds will have to be implemented to overcome these discrepancies in standards interpretations.

Because NG911 relies on GIS data for call routing, the GIS data must be highly accurate. It is recommended that the PSAP or 911 authority responsible for the GIS data today should ensure that it is of such quality so as to achieve a 98 percent or greater match rate with its legacy Master Street Address Guide (MSAG) and its GIS street centerline data before migrating to NG911. To accomplish this, the PSAP or 911 authority must have skilled GIS personnel on staff, or may elect to contract this task to a vendor that specializes in this type of work.

Model NG911 operating agreements, required between 911 authorities and service providers, do not exist. These agreements should cover subjects such as SLAs, incident management, problem management, change management, and network and system monitoring.

NG911 requires advanced call-handling systems and, in some cases, will require the PSAP to upgrade its call-handling system to accept the new call types.

PSAP logging and recording also will require change with the transition to an IP-based system.

Ancillary systems also may require upgrades to be compatible with NG911 call-handling systems. Such ancillary systems include, but are not limited to, CAD, MIS, and RMS.

NEEDS:

Nationwide leadership is needed to develop model NG911 operating agreements, required between 911 authorities and service providers.

Upgrade PSAP call-handling systems to accept new call types.

Update PSAP logging and recording devices to those that will support the transition to IP-based systems.

Improve broadband coverage nationwide.

Address incompatibilities between SIP versions implemented and service providers' systems.

Table C-1: Gaps and Needs of Architectural Characteristics, Feasibility, and Limitations of NG911 Summary

Gaps	Needs
Originating Service Environment	
Outside call centers such as poison control, language line service, N-1-1, and others will require upgrades to their systems and infrastructure in order to handle SIP calls. Operating agreements will be required between 911 authorities and service providers for gateways that may be required to connect these outside call centers to the PSAP network. SIP may not align properly between IMS and the i3 environment, and service providers may incur costs associated with transcoding SIP messaging exchanged between IMS and i3-compliant systems. The timeline for service provider network migration from TDM to SIP delivery varies widely and will impact both cost and ubiquity in the networks. Incompatibilities between versions of SIP implemented both by the service providers and by the 911 authorities cause a potential gap in the operational effectiveness of systems. Current location determination technologies used for identifying the location of wireless callers requires a substantial amount of time to provide a routable Phase II location.	Outside calls centers supporting PSAP operations should be engaged early in the planning process and their responsibilities clearly outlined. National guidance to develop model operating agreements is needed for 911 authorities and service providers that address requirements for outside call center connectivity in the network. Timelines and costs should be well understood between the 911 authority and the service provider(s). Carriers should continue to improve their location-determination technologies and the delivery of a dispatchable location to the PSAP with the call delivery.

Gaps	Needs
Core Services	
Core services cannot operate independently without transitional components, such as the OSE gateways discussed above. Until the full end-state transition is complete, this will continue to be a gap requiring transitional components. Transitional elements will be required while 911 authorities develop supporting GIS data, staff, and operational processes for the NENA i3 location-validation and geospatial call-routing functions. The NOC/SOC is required to have SOPs in place for notifying customers and the FCC NORS, and these SOPs are not yet developed. Interconnection agreements with OSPs and legacy 911 service providers will be required to enable the receipt and transfer of 911 calls. Examples of a well-defined SOW and strong SLAs needed to provide 911 authorities with assurances concerning the required level of service needs and system availability requirements do not exist. NG911 GIS maintenance requirements require extensive technical expertise. The expertise required to manage the complexity of planning and deploying these systems, and the high cost of transition presents a technical and funding gap.	Complete the development of supporting GIS data, staff, and operational processes for the NENA i3 location-validation and geospatial call-routing functions. Nationwide leadership is needed to develop model interconnection agreements between OSPs and legacy service providers, and SOW and SLA models for 911 authorities to follow. Local authorities will need to secure GIS expertise of the level necessary to support the critical nature of the 911 support systems. Nationwide leadership is needed to assist states and regions in securing sustainable funding to address the challenges of the transition and ongoing maintenance of NG911.

Gaps	Needs
PSAPs and Responders	
Model NG911 operating agreements, required between 911 authorities and service providers, do not exist. These agreements should cover subjects such as SLAs, incident management, problem management, change management, and network and system monitoring.	Nationwide leadership is needed to develop model NG911 operating agreements, required between 911 authorities and service providers.
NG911 requires advanced call-handling systems and, in some cases, will require the PSAP to upgrade its call-handling system to accept the new call types.	Upgrade PSAPs' call-handling systems to accept new call types.
PSAP logging and recording also will require change with the transition to an IP-based system.	Update PSAPs' logging and recording devices to those that will support transition to IP-based systems.
Ancillary systems also may require upgrades to be compatible with NG911 call-handling systems. Such ancillary systems include, but are not limited to, CAD, MIS, and RMS.	Improve broadband coverage nationwide.
Although broadband is considered to be widely deployed, there are areas in the country where it either is not deployed, or is deployed but with bandwidth limitations. The limitations may be due to distance, loop quality, or other factors.	Address incompatibilities between SIP versions implemented and service providers' systems.
Incompatibilities will exist between versions of SIP implemented both by the service providers and by the 911 authorities. Workarounds will have to be implemented to overcome these discrepancies in standards interpretations.	

C.2.   NG911 MATURITY MODEL DOMAIN ASSESSMENT

The NG911 Maturity Model consists of six domains consisting of functional and/or operational components. Each domain was reviewed to identify gaps within the applicable standards and best practices. The NG911 Maturity Model is described in detail in Appendix B.

Standards development is an ongoing and recurring process rather than a single event. Existing standards are evolving continually, and new standards are being implemented as technology is upgraded or new technologies are developed. Standards bodies develop and issue technical and operational standards applicable to telecommunications systems, as well as PSAP operations and systems. Such organizations include the following:

- Alliance for Telecommunications Industry Solutions (ATIS)
- Association of Public-Safety Communications Officials (APCO)
- Federal Bureau of Investigation (FBI)
- Federal Communications Commission (FCC)
- First Responder Network Authority (FirstNet)
- International Organization for Standardization (ISO)
- International Telecommunication Union (ITU)
- Internet Engineering Task Force (IETF)
- Institute of Electrical and Electronics Engineers (IEEE)
- National Emergency Number Association (NENA)
- Telcordia®
- Telecommunications Industry Association (TIA)
- 3rd Generation Partnership Project (3GPP)

Many of these standards bodies currently are involved with standards development for various elements of the NG911 systems and operations. The office publishes an annual report of the many standards and standards organization related to the NG911 systems.

C.2.1. BUSINESS DOMAIN

The Business Domain consists of planning and procurement activities required to lay the groundwork for a transition to NG911. While researching the functional and technical requirements of the Business Domain, a gap in best practices and standards related to national governance was identified.

To facilitate a nationwide transition to NG911, it will be necessary to have some level of nationwide governance, including the identification and adoption of national standards. There will be a need for states and regions to interconnect networks to transfer calls across borders, synchronize GIS files, and share data. Nationwide governance does not mean a federal agency

must dictate or oversee 911 operations; however, coordination is needed at the nationwide level to ensure that the full benefits of NG911 are realized.

GAP:

While there are best practice documents available, such as the National 911 Guidelines Assessment Report[65], to help states evaluate programs, governance and legislation, there are no guidelines for a nationwide level of coordination available today. In addition, and perhaps of more importance, no recommendations exist for achieving the level of nationwide coordination and assistance required to advance the implementation of NG911.

NEEDS:

Guidance is needed regarding the appropriate partners required to conduct a nationwide-level gap analysis in this area. Such an analysis should be performed to identify the areas that require nationwide-level governance to assist in the nationwide transition to NG911. Once a nationwide-level gap analysis is completed, a nationwide governance plan will be required to advance the nationwide transition to NG911. The nationwide governance plan would identify nationwide stakeholder groups, roles and responsibilities, authority levels, nationwide system oversight responsibility, the interrelationships of nationwide and local 911 authorities, and a model for interstate agreements needed to advance a nationwide seamless transition to NG911.

C.2.2. DATA DOMAIN

The Data Domain captures the data management responsibilities of PSAPs, states and nationwide authorities as they prepare for and implement NG911. In the NG911 Maturity Model, the Data Domain includes a shift from tabular location data to full dependency on GIS data for the verification of caller location and routing of 911 calls. The gap analysis in the Data Domain uses the End State standards as the desired goal, and the current standards status as the starting point.

---

[65] Draft Report for National 9-1-1 Assessment Guidelines," 911 Resource Center, June 2012, https://resourcecenter.911.gov/911Guidelines/RPT053012_National_911_Assessment_Guidelines_Report_FINAL.pdf.

GAP:

A gap exists as several NENA standards currently are undergoing revision and are not yet finalized. Those that are related to this section are NENA 08-003[66] (i3) and NENA 02-014[67] (GIS Data Collection & Maintenance). Release dates are not yet set for the new versions; both will be issued with a new document number.

NEEDS:

While current versions of these standards are sufficient for early planning and deployments through the Transitional stage, until the standards are finalized and accepted by the 911 community and industry, a lack of clear direction will exist and implementation will lag as agencies fear stranded investment and what might change in the final version of a standard.

C.2.3. APPLICATIONS AND SYSTEMS DOMAIN

The Applications and Systems Domain is used to describe the applications, systems and other core functions of NG911 systems. The gap analysis used current standards status as the starting point, and the End State standards as the desired goal.

The NENA standards pertinent to the Applications and Systems Domain are NENA 08-003 (i3) and NENA 75-001[68] (NG Security), and both currently are undergoing revision. Release dates are not yet set for the new versions; both will be issued with a new document number.

Integrated logging systems fall under the Applications and Systems Domain. While identifying standards related to integrated logging, it was discovered that the Session Recording Protocol (SIPREC) RFC[69] 7866 was published by the IETF in May 2016, but the standard is not well established.

---

[66] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, https://www.nena.org/?page=i3_Stage3.
[67] "GIS Data Collection & Maintenance," National Emergency Number Association, July 7, 2007, http://www.nena.org/?page=gisdatacollection.
[68] "Security for Next-Generation 9-1-1, National Emergency Number Association, February 6, 2010, https://www.nena.org/?page=NG911_Security.
[69] Request for Comments

GAP:

A gap exists because the necessary Applications and Systems Domain-related standards and informational documents that will assist moving NG911 implementation forward are not complete and a final release is not defined.

NEEDS:

Complete the NENA i3 standard (NENA 08-003 [i3]). Complete the NENA roadmap for solution providers.

C.2.4. INFRASTRUCTURE DOMAIN

The Infrastructure Domain is used to describe the infrastructure elements that interconnect the NGCS of the Applications and Systems Domain elements. The gap analysis used the current standards as the starting point, and the End State standards as the desired goal.

The basic IETF and IEEE standards applicable to IP networks have been in place for many years. Network devices and systems that communicate with each other at a basic IP level may be deemed to meet the basic IP network standards. These standards include, but are not limited to the following:

- Session Initiation Protocol (SIP)
- Hypertext Transfer Protocol (HTTP)-Enabled Location Delivery (HELD)
- Location-to-Service Translation (LoST)
- Real-Time Transport Protocol (RTP)
- Transport Layer Security (TLS)
- Message Session Relay Protocol (MSRP)

The SIP messaging and RTP media-streaming standards have been in place for some time and are stable. Any changes to the standards will involve additional features or functionality over and above the currently developed standards.

Several NENA standards are undergoing revision. Standards applicable to this section are NENA 08-003 (i3), NENA 08-506[70] (IP Network Design for NG911) and NENA 75-001 (NG Security). Release dates are not yet set for the new versions.

---

[70] "Emergency Services IP Network Design for NG9-1-1," National Emergency Number Association, December 14, 2011, https://www.nena.org/?IP_Network_NG911.

While identifying standards for the ESInet, it became apparent that although NENA does not have a specific standards document for ESInets that has progressed through its standards process, it has issued an informational document for ESInet design, NENA 08-506 (Emergency Services IP Network Design for NG911), which provides a high-level concept of emergency service networks that 911 authorities have used absent a standard. This document currently is being revised. An end state for the revision completion has not been defined.

It also is important to note that the standards for interconnected IP networks are well-established, implemented, and tested. The underlying protocols—including, but not limited to, Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Bidirectional Forwarding Detection (BFD), Differentiated Services Code Point (DSCP), and SIP—are stable. Installation technicians and support engineers are well-versed in the configuration, troubleshooting, and maintenance of the network devices and protocols used in the construction of the IP network.

To support NOC network monitoring, the Simple Network Management Protocol (SNMP) is at Version 3, but that version is not as widely supported as the previous version, Version 2. Version 3 includes cryptography functionality to improve security of the management systems, but many devices do not yet support the cryptography.

Today's PSAPs use well-established land mobile radio (LMR) and wireless data systems to exchange information with emergency responders. The LMR standards have been in place for a long time and are considered stable. Wireless data standards also are stable, but are evolving as lessons are learned through system deployments, or as technology is upgraded or developed. In the future, such systems likely will be integrated with those being deployed by FirstNet. FirstNet continues to develop and update its network policies that provide guidance on technical and operational requirements for data access and exchange, network interfaces, and network security, including intercarrier connections.

GAP:

NENA's informational document for ESInet design, NENA 08-506 (Emergency Services IP Network Design for NG911) currently is being revised. An end state for the revision completion has not been defined. Also, SNMP V3 is not extensively supported because many devices to do support cryptography. FirstNet technical and operational requirements are still under development, and additional coordination between FirstNet and NG911 is needed. FirstNet technical and operational requirements will be updated continually to meet public safety's ever-changing needs, and coordination between FirstNet and NG911 will be a continual effort.

NEEDS:

Complete the NENA standards. Complete FirstNet technical and operational requirements. Work to achieve support for the SNMP V3 standard. Work with FirstNet to evolve technical and operational requirements, and coordinate the interconnection requirements and standards between NG911 and FirstNet.

C.2.5. SECURITY DOMAIN

The Security Domain encompasses the network, facility, and personnel security associated with the implementation of NG911 services. This domain focuses on the systems and applications required to develop a security framework appropriate for each stage of the NG911 Maturity Model. As with other domains the gap analysis for the Security Domain used the current standards as the starting point, and the End State standards as the desired goal.

GAP:

A gap exists because several NENA standards are undergoing revision and are not yet complete. Those applicable to this section are NENA 08-003 (i3), NENA 08-506 (Emergency Services IP Network Design for NG911), and NENA 75-001 (NG Security). Release dates are not yet set for the new versions.

NEEDS:

Complete the NENA i3 standard and other related informational documents and standards

C.2.6. OPERATIONS/PERFORMANCE DOMAIN

The Operations/Performance Domain is used to describe the policies, procedures, and programs that are needed to effectively operate NG911 systems.

While gathering information on the functional and technical requirements, a gap was identified concerning automated data analytics. Data analytics refer to qualitative and quantitative techniques and processes used to enhance productivity, functional effectiveness, and operational understanding. Data is extracted from a variety of sources and categorized to identify and analyze behavioral data and patterns. In the 911 environment, data analytics currently are a challenge because of the proprietary and silo nature of the components comprising the present system(s). NG911 promises to bring a large amount of data to the public safety system. Getting the right data to the right people at the right time will enhance the operational effectiveness and system

functionality. Data analytics can provide a means for the system(s) to process large amounts of data based on the needs of the system participants.

GAP:

The gap in the Operations/Performance Domain is that no standards or best practices currently exist for 911 authorities to reference when making decisions, or when developing standards and procedures regarding the use of data analytics in the 911 environment.

NEEDS:

A suggested best-practices document related to data analytics application in the PSAP, as well as operational standards and effective practices for use of data analytics is needed to assist 911 authorities in the effective operation of NG911 systems.

Table C-2: NG911 Maturity Model Domain Gaps and Needs Summary

Gap	Needs
Business Domain	
Best-practices documents to help states evaluate programs, governance and legislation are available; however, there is no documentation assessment for assessing the nationwide level of coordination.

No recommendations exist for achieving the level of nationwide coordination and assistance required to advance the implementation of NG911. | Guidance is needed regarding the appropriate partners required to conduct a nationwide-level gap analysis in this area.

Analysis should be performed to identify the areas that require nationwide governance to assist in the nationwide transition to NG911.

A nationwide governance plan is required to advance the nationwide transition to NG911.

The nationwide governance plan should identify stakeholder groups, roles and responsibilities, authority levels, system oversight responsibility, the interrelationships of national and local 911 authorities, and a model for interstate agreements needed to advance a nationwide seamless transition to NG911. |
| **Data Domain** | |
| NENA standards currently are being revised and are not yet finalized. Those that are related to this section are NENA 08-003[71] (i3) and NENA 02-014[72] (GIS Data Collection & Maintenance).

Release dates are not yet set for the new versions. | Finalize the standards setting and acceptance process. |

---

[71] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, https://www.nena.org/?page=i3_Stage3.

[72] "GIS Data Collection & Maintenance," National Emergency Number Association, July 7, 2007, http://www.nena.org/?page=gisdatacollection.

Gap	Needs
Applications and Systems Domain	
The necessary Applications and Systems Domain-related standards and informational documents are not complete and a final release is not defined.	Complete the NENA i3 standards to include (NENA 08-003 [i3]), the NENA INF XXX roadmap for solution providers, and other updates to existing standards.
Infrastructure Domain	
NENA informational document for ESInet design, NENA 08-506 (Emergency Services IP Network Design for NG911) currently is being revised. An end state for the revision completion has not been defined. Also, SNMP V3 is not extensively supported because many devices do not support cryptography. FirstNet technical and operational requirements are still under development.	Complete NENA standards. Complete FirstNet technical and operational requirements. Work to achieve support for SNMP V3 standard.
Security Domain	
NENA standards are being revised and are not yet complete. Those applicable to this section are NENA 08-003 (i3), NENA 08-506 (Emergency Services IP Network Design for NG911), and NENA 75-001 (NG Security). Release dates are not yet set for the new versions.	Complete the NENA i3 standard and other related informational documents and standards.
Operations/Performance Domain	
No standards or best practices exist for 911 authorities to reference when making decisions, or when developing standards or procedures for the use of data analytics in the 911 environment.	No standards or best practices exist for 911 authorities to reference when making decisions, or when developing standards or procedures for the use of data analytics in the 911 environment.

C.3. NG911 SERVICE NEEDS FOR FUNCTIONAL NEEDS COMMUNITY ASSESSMENT

The number of individuals experiencing 911 access challenges covers a wide spectrum of the population. The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 4B[73] referenced the Individuals with Disabilities Education Act[74] (IDEA), which defines 13 categories of disability:

- Autism
- Deaf-blindness
- Deafness
- Emotional disturbance
- Hearing impairment
- Intellectual disability
- Multiple disabilities
- Orthopedic impairment
- Other health impairment
- Specific learning disability
- Speech or language impairment
- Traumatic brain injury
- Visual impairment, including blindness

In addition, CSRIC included two additional groups:

- Elderly
- Non-English speakers (i.e., Chinese, English, French, Spanish, Native American languages, etc.).

U.S. Census Bureau statistics identity that**: "**There are 54.4 million Americans who have disabilities, and 35 million Americans who have a severe disability. For those aged 15 and older, this includes 7.8 million who have difficulty seeing the words in ordinary newsprint; 7.8 million who have difficulty hearing a typical conversation; 2.5 million who have difficulty having their speech understood; 27.4 million who have lower body limitations; 19 million with upper body limitations; and 16.1 million with cognitive, mental and emotional functioning disabilities."[75]

---

[73] CSRIC, *Working Group 4B Transition to Next Generation 9-1-1 Final Report*, (March 2011), Federal Communications Commission, http://transition.fcc.gov/pshs/docs/csric/CSRIC-WG4B-Final-Report.pdf.

[74] Individuals with Disabilities Education Act, https://sites.ed.gov/idea/.

[75] Elizabeth E. Lyle, *A Giant Leap & A Big Deal: Delivering on the Promise of Equal Access to Broadband for People with Disabilities—OBI Working Paper Series No. 2*, (April 2010), Federal Communications Commission,

The National Institute on Deafness and Other Communication Disorders (NIDCD) reports that approximately 15 percent of American adults (37.5 million) report some trouble hearing.[76] In addition, approximately 38 million Americans (12.4 percent of the total population) are older than age 65 (United States Census Bureau, 2008) and represent a population that frequently faces many of the same limitations as people with disabilities. It is predicted that the population aged 65 and older will more than double between 2012 and 2060, from 43.1 million to 92.0 million.[77]

People with disabilities currently face various barriers in communicating with the legacy 911 system and potentially will encounter similar issues with future NG911-capable PSAPs.[78] The Emergency Access Advisory Committee (EAAC) Report on Emergency Calling for Persons with Disabilities Survey Review and Analysis 2011, emphasized the following two critical issues:

- 83 percent of respondents indicated that it was very important that they be able to call 911 using the same device (i.e., using text, video, voice, and/or captioned telephone) that they use to typically communicate every day.[79]
- 77 percent of respondents emphasized that it was very important to call 911 directly rather than via relay service.[80]

According to the FCC Telecommunications Relay Services (TRS) reports, teletypewriter (TTY) usage decreased more than 80 percent between 2008 and 2015. During the same period, a significant upward trend occurred regarding use of Internet Protocol Captioned Telephone Service (IP CTS) and Video Relay Service (VRS).[81] IP CTS enables people who can use their own voice, but have difficulty hearing when on a call, to engage in a telephone conversation using an IP-enabled device that allows them to listen or talk to the other party and read captions of what the other party is saying, similar to hearing and voice carry-over with TTY today.

---

http://download.broadband.gov/plan/fcc-omnibus-broadband-initiative-(obi)-working-report-giant-leap-big-deal-delivering-promise-of-equal-access-to-broadband-for-people-with-disabilities.pdf.

[76] "Quick Statistics About Hearing," National Institute on Deafness and Other Communication Disorders, December 15, 2016, https://www.nidcd.nih.gov/health/statistics/quick-statistics-hearing.

[77] "U.S. Census Bureau Projections Show a Slower Growing, Older, More Diverse Nation a Half Century from Now," United States Census Bureau, December 12, 2012, https://www.census.gov/newsroom/releases/archives/population/cb12-243.html.

[78] The Emergency Access Advisory Committee, *Working Group 3 Recommendations on Current 911 and Next Generation 911: Media Communication Line Services Used to Ensure Effective Communication with Callers with Disabilities*, (March 1, 2013).

[79] The Emergency Access Advisory Committee, *Report on Emergency Calling for Persons with Disabilities Survey Review and Analysis,* 2011, https://transition.fcc.gov/cgb/dro/EAAC/EAAC-REPORT.pdf, question #23 on page 30.

[80] Ibid., question #22 on page 29.

[81] "Federal TRS Reports," Roulka Loube, http://www.rolkaloube.com/formsreports. Comparable figures for August 2008 were approximately 70,000 IP CTS monthly minutes and 7.5 million monthly VRS minutes.

While the statistics from the TRS reports indicate a significant decline in TTY usage, it cannot be assumed that TTY is no longer required. Rather, it is important that the NG911 environment continues to provide TTY capability. However, transmitting the Baudot tones used in TTY communications over an IP network can be challenging. NENA 08-003 (i3) calls for a transcoder in the path of every voice call to translate Baudot tones going into the PSAP, and to synthesize them on the way out of the PSAP.[82]

In addition, there is a need to allow the communication preferences of a 911 caller to be:
- Transmitted with the call
- Understood within the NG911 core environment
- Used to process the call

An example is the ability to bridge in the appropriate third party—such as IP CTS, a relay service, or a language line service—at the time of call. This ability would allow the caller to provide a language preference in addition to any communications technology preference. The NENA i3 architecture identifies this ability, but the process for using any or all of the available data is still in development, creating another gap to be addressed.

The EAAC recommends that Media Communication Line Services (MCLS) be established to facilitate 911 calls in the NG911 environment, to enable individuals with disabilities to make direct 911 video calls using different communication modalities. The MCLS must be capable of providing direct access to NG911 for individuals with disabilities who make video, text, and voice calls, and must include the ability to communicate in sign language, speech-to-speech, text-to-voice, voice-to-text or any combination thereof by:
- A direct 911 call rather than through third-party relay services
- Usage of multimedia communication technologies
- Multi-party conferencing via a bridge call

Both MCLS call centers and PSAPs need to adhere to pertinent standards for NG911 to be fully interoperable.[83]

Finally, there will be a need to train PSAP staff on the various methods that individuals with disabilities have available to directly access the PSAP. On the outbound, or egress, side of the NG911 network, there will be a need to train the PSAP staff on how to manually bridge the call to third-party services needed to process communication with the individual with disabilities. Until

---

[82] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, http://www.nena.org/?page=i3_Stage3, section 4.1.8.4.

[83] The Emergency Access Advisory Committee, *Working Group 3 Recommendations on Current 911 and Next Generation 911: Media Communication Line Services Used to Ensure Effective Communication with Callers with Disabilities*, (March 1, 2013).

the system has the ability to automatically bridge in third-party services, the PSAP staff will need to perform that task as quickly and efficiently as possible. In addition, until language translation is able to be automatically bridged in by the NG911 system at the time of call, there will be challenges related to translations for text and other media. Current SOPs and training will need to be updated by PSAPs to include NG911 accessibility options.

GAP:

There is currently a focus on deploying text-to-911 service, and several interim solutions are being implemented throughout the country. However, several additional areas require nationwide-level coordination to facilitate not just text-to-911, but also equal access to NG911 technologies. Although best-practices documents for implementing text-to-911 service exist, nothing has been written regarding the implementation of other NG911 capabilities such as video, pictures or sensors, even though communication technologies in general are changing rapidly and expanding, and this gap has been noted by the Team. The result is that individuals with disabilities are taking advantage of these advancements to meet their personal communication needs, but they cannot use the same technologies to access 911 services.

NEEDS:

To facilitate a nationwide transition to NG911, it will be necessary to have nationwide guidance for the creation of standards and best practices regarding multimedia services that will be employed in the NG911 environment.

C.4.   ACCESS TO BROADBAND

Twice a year, the FCC collects data from broadband providers in the U.S. to identify access to both fixed and mobile broadband services. This data is used to compile an annual broadband progress report.

According to the FCC's 2016 Broadband Progress Report[84], while the nation continues to make progress in broadband deployment, many Americans still lack access to advanced, high-quality voice, data, graphics and video offerings, especially in rural areas and on tribal lands.

The report finds that 34 million Americans—10 percent of the population—lack access to advanced broadband service. Moreover, a significant digital divide remains between urban and rural America, as almost 40 percent of all rural Americans lack access to 25 megabits per second

---

[84] "2016 Broadband Progress Report," Federal Communications Commission, January 29. 2016, https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report.

(Mbps) (download) and 3 Mbps (upload) service. In contrast, only 4 percent of urban Americans lack access to 25 Mbps/3 Mbps broadband.

This lack of broadband access impacts public safety's NG911 readiness and ability to implement ESInets, or managed IP networks used for emergency services communications that can be shared by all public safety agencies.[85] Providing a cost-effective IP network to connect the PSAPs in a state or region is proving problematic in areas with limited or no broadband access. The 911 industry is seeing regional ESInets more easily deployed in metropolitan areas, but less so in rural areas.

In addition, questions about the regulatory environment and liability concerns are causing a roadblock for the NG911 transition. After instances of statewide outages gathered national attention, questions have been raised about 911 technical and regulatory enforcement in an environment of interconnected vendors. Some broadband providers recently have indicated an unwillingness to provide service to the 911 sector due to these concerns. In rural areas with limited broadband access, this is proving to be a roadblock for the NG911 transition. Resolving these issues may require changes in public policy.

C.4.1. FCC'S 2016 BROADBAND PROGRESS REPORT OVERVIEW OF DATA

All facilities-based broadband providers are required to file data with the FCC twice a year (Form 477) regarding where they offer Internet service at speeds exceeding 200 kilobits per second (kbps) in at least one direction. The FCC collects data from fixed and mobile data service providers. Fixed providers use physical networks to provide direct, wired broadband access from service supplier to service user. Fixed providers file lists of census blocks in which they can or do offer service in at least one location, with additional information about the service.

Mobile providers offer wireless broadband access through a portable modem, mobile phone, USB wireless modem, tablet, or other mobile devices. Mobile providers file maps of their coverage areas for each broadband technology, e.g., Evolution-Data Only (EV-DO), High-Speed Packet Access (HSPA), and Long-Term Evolution (LTE).

The maps on the following pages provide a snapshot illustration of the FCC's findings described in the 2016 Broadband Progress Report.

The FCC's Wireline Competition and Wireless Telecommunications bureaus released data on fixed broadband deployments as of June 2016.

---

[85] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, http://www.nena.org/?page=i3_Stage3.

This data was collected through FCC Form 477 and is available on the Commission's Broadband Deployment Data webpage.[86] This data will be used to produce future FCC broadband progress reports.
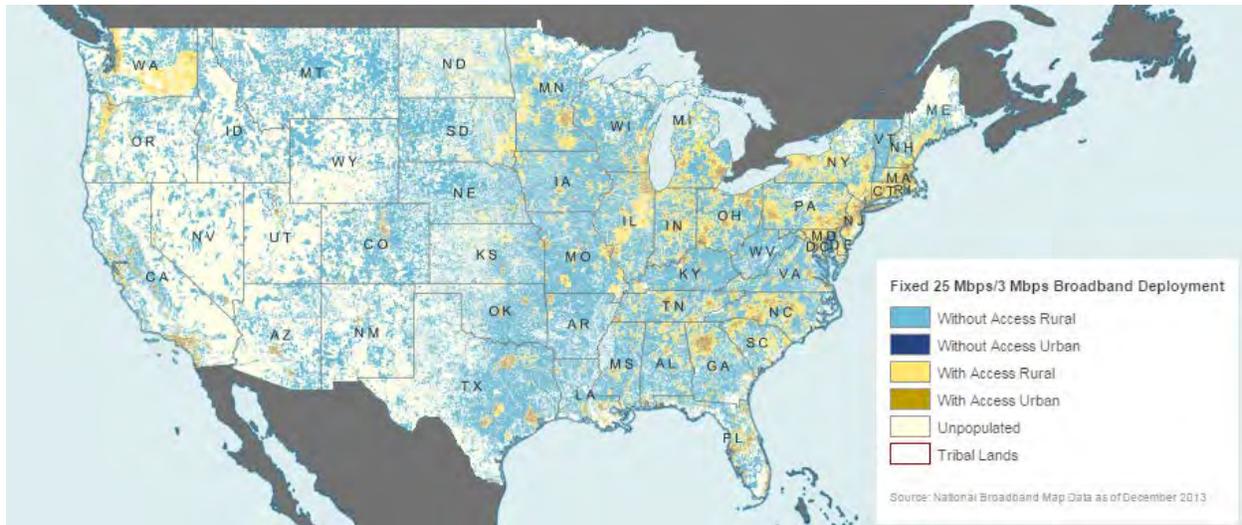
Figure C-1: Fixed 25 Mbps/3 Mbps Broadband Deployment Map

This map illustrates the Commission's fixed broadband deployment results described in the 2016 Broadband Progress Report; it relies on data from the National Broadband Map as of June 2016. It shows areas of the U.S. where fixed residential broadband services of at least 25 Mbps download and 3 Mbps upload are deployed, and where such services are not deployed.

---

[86] "Fixed Broadband Deployment Data from FCC Form 477," Federal Communications Commission, June 30, 2016, www.fcc.gov/encyclopedia/broadband-deployment-data-fcc-form-477.
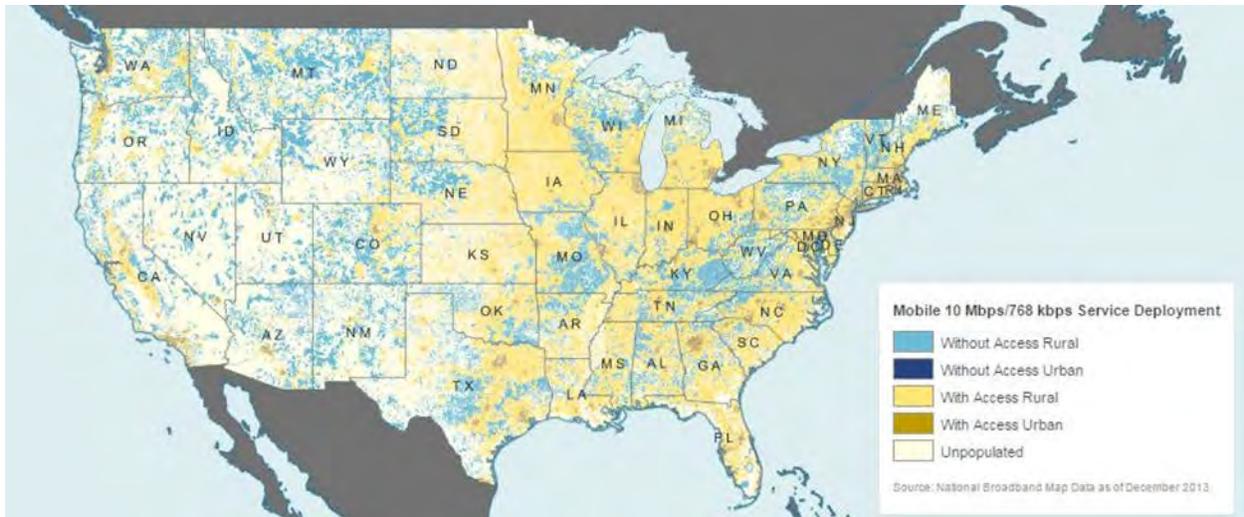
Figure C-2: Residential Fixed Broadband Providers at 25 Mbps/3 Mbps Map

This map shows the number of providers offering residential broadband services of at least 25 Mbps download and 3 Mbps upload. Areas without population are shown without color.

For more information on the data and definitions used in these maps, or on the 2016 Broadband Progress Report, visit https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report.

The report concludes that more work needs to be done by the private and public sectors to expand robust broadband to all Americans in a timely manner.

This page is intentionally left blank.

APPENDIX D – MATURITY MODEL ASSUMPTIONS AND DATA SOURCES

D.1. GENERAL ASSUMPTIONS

D.1.1. COST MODELING

Microsoft Excel was the primary tool used for modeling the cost study. The model documents data sources and allows traceability of the inputs, calculations, and modeling assumptions for document verification and validation. The model is a build-up/bottom-up estimate in which costs are estimated at the element level and then aggregated up to functional component and domain level costs.

One-time and recurring costs, as well as hardware refresh costs, for each element are applied at the stage for which the transition initially must occur, even if an element continues through multiple stages. For example, in Figure D-1, Applications and Systems Domain, Call Routing Functional Component, the IP Selective Routing element begins in the foundational stage and continues to the transitional stage. In this case, all one-time costs associated with the IP Selective Routing element will be applied to the Foundational stage and there will be no additional one-time costs in the Transitional stage. The recurring costs, as well as the hardware refresh costs, also are included within this element cost.
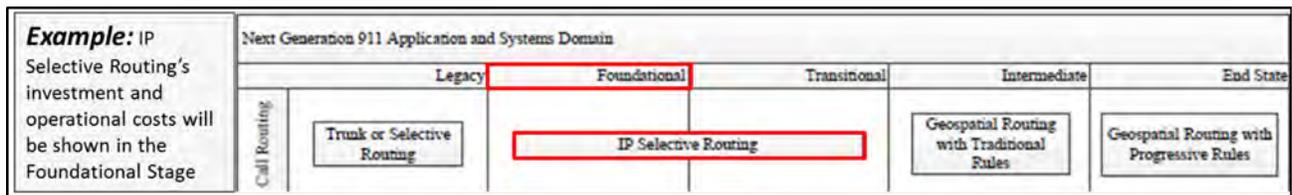
Figure D-1: Cost Distribution Example

The core cost estimation model is conducted by exercising a few high-level steps to generate total cost and repeating them for each geographic area. The overall cost estimation methodology for each cost type within every element is illustrated in Figure D-2 below.

Overall Cost Estimation Methodology for Cost Type within an Element			
Unit Cost ✗	Quantity ✗	Scale ✗	Factors ＝ Total Unadjusted One-time or Recurring Cost
Labor Rates	Workstations	Local	Redundancy factor
Equipment	FTE	Regional	Equipment Installation
*Normalized CY17 $s	Population	State	HW/SW O&M
*one-time or recurring	Number of PSAPs/Cores	National	HW/SW Modification Factors

Total Unadjusted One-time or Recurring Cost ✗	Progress ✗	Schedule ✗	Inflation ＝ 10-year Incremental Cost
	1-heatmap	4 or 6-year Investment	
	Adjusted one-time or recurring	Annual Operations	

Figure D-2: Cost Modeling Methodology

The normalized individual costs for each cost type within an element are used to calculate a one-time unit cost or an annual recurring cost. The costs used in the model vary based on the specific cost type and element. Some examples of costs are labor rates, individual hardware equipment cost, software licensing fees, office space cost (per square foot), and annual service fees.

The unit cost of each element is escalated to the local, regional, state, or national level by being multiplied by the identified quantity and scale. Each element has a unique scaling factor based on previously established assumptions. Some scaling factor examples are number of positions and workstations, number of full-time equivalent (FTE) staff, population, number of PSAPs, number of core data centers, etc.

For some CES, an additional factor is multiplied by the unit cost to account for other fees. For example, a hardware installation factor is applied to the acquisition cost of equipment to account for shipping, handling, and other service fees. Similarly, hardware and software operation and maintenance (HW/SW O&M) factors, as well as refresh and upgrade factors, are applied to appropriate unit costs.

To accurately account for any activities that have been put in place before the period of analysis for this cost study, the total cost of a specific Cost Element Structure (CES) is adjusted based on the expected progress for each area. The cost model applies the appropriate expected progress at the functional component level to each element's estimation. For example, if the current status of an NG911 functional component has a value of 70 percent in its legacy stage, this means that 70 percent of the population is covered by the systems that meet the definition of the maturity model for that stage. Therefore, 70 percent of any planning, acquisition, or implementation activities required for that area already have been in place at the time of this analysis. Hence, only the

remaining 30 percent require those systems. The total estimated cost for each element within that functional component then is adjusted to account only for 30 percent of the total cost. This is the portion of the total cost that is required to bring the entire area to the next stage.

Finally, the total ten-year adjusted cost for each element is phased based on that area's start year and the applicable functional component implementation schedule. For cost types with one-time costs, the implementation schedule is applied directly. For cost types with recurring operations or annual service charges, an adjusted schedule is utilized. All assumptions regarding the implementation schedule and operation schedule are discussed in Section D.1.7, Implementation Schedule Assumptions, of this Appendix. All incremental costs are reported in then-year dollars (i.e., adjusted for nominal inflation).

Estimation of total adjusted cost for each cost element is repeated for each area. This provides the basic information required for extrapolation of the analysis to a nationwide-level estimate of costs. However, it is recognized that NG911 policies and implementation characteristics (e.g., choosing between hardware procurement and service model) vary widely between states and territories within the U.S. The estimated multistate costs are aggregated to a national level and reported based on the ten FEMA regions.

D.1.2. ECONOMIC ASSUMPTIONS AND MODELING PARAMETERS

Table D-1 summarizes three essential components for defining specific economic parameters: scope of the analysis, parameter, and source. External economic factors—such as inflation rate, labor rate, and locality factor categories—also are summarized in the table. Economic assumptions are derived from federal government sources, and some are adjusted for regional application, such as labor rates. Discussion on how each parameter is used in the cost model is detailed in various sections of this report.

Table D-1: NG911 Lifecycle Cost Estimation (LCCE) Economic Parameters

Scope of Analysis	Parameter	Source
Geographic Scope	Entire U.S. divided in geographical regions/ municipalities based on FEMA Regional Offices	FEMA Regional Offices
Time Period of Analysis	Year 0 (NG911 current status): Year 1 - Year 10	SME Input
Base Year	2017	Booz Allen Estimate

Scope of Analysis	Parameter	Source
Inflation Rate[87]	Nominal and real discount rates for 10-year analysis per Office of Management and Budget (OMB) guidance	OMB A-94 Appendix C
Guidelines	LCCE methodology	GAO [88] Cost Assessment Guide and FHWA Life Cycle Analysis Primer Guidance[89]
Labor Rate Category and Locality Factors	Federal wage system schedule, contractor/vendor wages, local public safety personnel wages, and default to GS-10	Office of Personnel Management (OPM) labor rates[90], including benefits and fringe, and General Schedule Locality Pay[91]
Bandwidth Link Redundancy Factor	2	SME Input
Hardware Device Redundancy Factor	1.5	SME Input
Hardware and Software Maintenance	15%	Booz Allen Estimate
Software Upgrade	10%	Booz Allen Estimate
Hardware Installation	50%	Booz Allen Estimate
Hardware Refresh Cycle	5 years	Booz Allen Estimate

D.1.3. PERIOD OF ANALYSIS AND INFLATION ASSUMPTIONS

Inflation rate accounts for the sustained increase in the general level of prices in the economy. Historical cost data collected for this study are escalated to adjust for inflation to estimate future costs. Previous year collected costs are normalized to a base year to account for historical inflation. The estimating approach using these 2017 constant year values is summarized below.

---

[87] The inflation rate, approximately 1.88%, is based on the ratio between the real and nominal discount rates for a 10−year analysis as allowed for within Office of Management and Budget (OMB) Circular A-94, Appendix C, as of November 2015.

[88] Government Accountability Office, *GAO Cost Estimating and Assessment Guide Best Practices for Developing and Managing Capital Program Costs*, (March 2009), http://www.gao.gov/new.items/d093sp.pdf.

[89] U.S. Department of Transportation, *Life-Cycle Cost Analysis Primer*, (August 2002), https://www.fhwa.dot.gov/asset/lcca/010621.pdf.

[90] "Pay & Leave," Office of Personnel Management, 2016, https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2016/general-schedule/.

[91] "General Schedule (GS) Locality Pay Map," FederalPay.org, https://www.federalpay.org/gs/locality.
"Search awarded ceiling rates for labor categories," Contract-Awarded Labor Category, https://calc.gsa.gov/.
IT Schedule 70.

- All historical data are escalated to the 2017 base year.
- Unit costs are estimated in this base year for the purpose of developing cost element relations (CERs) and other estimating methodologies.
- Estimated total costs are spread using time-phasing methodologies based on the implementation schedule resulting in an obligation profile.
- Base year costs in each time period (year of analysis) are escalated to then-year dollars using that year's proper inflation index.
- The total ten-year cumulative costs presented in this report are all inflation-adjusted dollars for a ten-year period of analysis.

D.1.4. LOCALITY FACTOR AND LABOR RATES ASSUMPTIONS

This cost study considers activities performed by both government and contractor staff. Rather than developing a specific rate schedule for estimating government staffing efforts within each region, the General Schedule (GS) labor rate grades are used as the approximation for individual regions' government labor rates. The fully loaded GS labor rates used in the model include all overhead and fringe benefit costs, and a regional locality factor is applied. The GS-10 grade has been set as the default labor rate for all technical/managerial efforts. This assumption is changed and the labor rate is adjusted for elements that require significantly higher technical levels of expertise. In addition to government labor rates, four common labor categories and salaries for contractors are identified and utilized in the cost study. These values were developed from the GSA Contract Awarded Labor Category (CALC) dataset, which utilized an average of all similar labor categories and descriptions of between 8–15 years of experience for Telecommunication Systems Engineer, Network Engineer, Policy Planner, and Emergency Systems Planner. The GS and contractor labor rates are summarized in Appendix D, Section D.8, Reference Tables, Table D-33.

D.1.5. SUSTAINMENT COST FACTORS

This full ten-year LCCE cost analysis includes costs for hardware and systems software annual maintenance and technology refresh cycles. The specific assumptions and parameters used to address the annual maintenance and equipment refresh cycles are listed below.

- For any CES with a hardware cost type, an additional hardware installation cost (i.e., 50 percent of the total hardware acquisition) is included to account for delivery, installation, acceptance testing, and any other engineering and support fees.
- Any hardware suite or office equipment procured during the period of this analysis is assumed to have a useful life of five years. A full hardware refresh cost (i.e., 100 percent of the total acquisition cost) is applied at the end of that equipment's useful life. This

technology refresh cycle of every five years is applied to appropriate CES based on their specific implementation schedule.

- An annual O&M cost also is included for all purchased software licensing and hardware. The O&M annual cost is assumed to be 15 percent of the total procurement cost based on industry standards. The annual O&M cost for each element is applied starting one year after the investment year based on its specific implementation schedule.
- Any O&M costs for hardware or software procured before the start year of this analysis, based on the NG911 current status, are not accounted for in this study. Capturing the ongoing O&M expenses for equipment and software licensing purchased before the start year of this analysis is out of scope. However, as the hardware refresh of existing equipment is included, when the refresh occurs, future O&M is adjusted to the complete hardware procurement cost.

D.1.6. IMPLEMENTATION SCHEDULE ASSUMPTIONS

To determine a likely NG911 overall deployment schedule and cost, an implementation timeline and start year are defined for each area. Achieving the desired NG911 End State is scheduled for all states and territories within ten years of initiation. The NG911 current status is estimated at Year 0 (current state of NG911); by the end of Year 10, the entire nation is assumed to be at the defined end state. The implementation schedule only applies to investment costs. Operational costs will occur in subsequent years of each individual investment. Based on these assumptions, the nation will be at end state by the end of Year 10, given the following conservative assumptions:

- No scheduling delays;
- No funding delays; and
- No deviations from the recommended implementation path.

Each area is assigned a start year by SMEs, which is based on that area's current NG911 readiness. To ensure a nationwide deployment within ten years, all assigned start years begin within the first four years of the implementation timeline. In addition, each region follows one of two default implementation options: a four-year or six-year schedule.

States that have a strong coordination authority and governance in place likely will take less time than those that need to develop the coordination and governance. The study estimates that about 46 percent of the states have strong coordination in place based on responses to the National Profile Database and FCC funding report. These states are estimated to be able to deploy in four years. The remainder are estimated to take six years.

Similar to the deployment year, the schedule is assigned by SMEs, and is based on the area's current NG911 readiness. Table D-2 illustrates how the costs associated with each stage of each domain are phased based on a four-year or a six-year schedule.

Table D-2: Four-year and Six-year Implementation Schedules

4 Year Implementation Schedule					
Domain	Stage	Yr 1	Yr 2	Yr 3	Yr 4
Business	Foundational	100%	--	--	--
Business	Transitional	--	100%	--	--
Business	Intermediate	--	--	100%	--
Business	End State	--	--	--	100%
Data	Foundational	50%	50%	--	--
Data	Transitional	--	50%	50%	--
Data	Intermediate	--	--	50%	50%
Data	End State	--	--	--	100%
Applications	Foundational	50%	50%	--	--
Applications	Transitional	--	--	100%	--
Applications	Intermediate	--	--	50%	50%
Applications	End State	--	--	--	100%
Infrastructure	Foundational	--	40%	60%	--
Infrastructure	Transitional	--	20%	80%	--
Infrastructure	Intermediate	--	--	30%	70%
Infrastructure	End State	--	--	--	100%
Security	Foundational	--	20%	80%	--
Security	Transitional	--	--	50%	50%
Security	Intermediate	--	--	--	100%
Security	End State	--	--	--	100%
Operations	Foundational	--	--	50%	50%
Operations	Transitional	--	--	50%	50%
Operations	Intermediate	--	--	50%	50%
Operations	End State	--	--	50%	50%

6 Year Implementation Schedule							
Domain	Stage	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5	Yr 6
Business	Foundational	75%	25%	--	--	--	--
Business	Transitional	--	50%	50%	--	--	--
Business	Intermediate	--	--	100%	--	--	--
Business	End State	--	--	--	100%	--	--
Data	Foundational	--	25%	25%	25%	25%	--
Data	Transitional	--	--	50%	50%	--	--
Data	Intermediate	--	--	33%	33%	33%	--
Data	End State	--	--	--	--	50%	50%
Applications	Foundational	--	50%	50%	--	--	--
Applications	Transitional	--	--	100%	--	--	--
Applications	Intermediate	--	--	33%	33%	33%	--
Applications	End State	--	--	--	33%	33%	33%
Infrastructure	Foundational	--	40%	60%	--	--	--
Infrastructure	Transitional	--	--	50%	50%	--	--
Infrastructure	Intermediate	--	--	33%	33%	33%	--
Infrastructure	End State	--	--	--	33%	33%	33%
Security	Foundational	--	--	50%	50%	--	--
Security	Transitional	--	--	33%	33%	33%	--
Security	Intermediate	--	--	--	50%	50%	--
Security	End State	--	--	--	33%	33%	33%
Operations	Foundational	--	--	50%	50%	--	--
Operations	Transitional	--	--	50%	50%	--	--
Operations	Intermediate	--	--	--	33%	33%	33%
Operations	End State	--	--	--	--	50%	50%

D.1.7. NG911 CURRENT STATUS ASSUMPTIONS

The overall NG911 Maturity Model's current status at the domain level, shown in the current environment Section 3 and Appendix B, was developed to measure the current status of NG911 nationwide. The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage. The NG911 current status is a snapshot of NG911 implementation from which the cost model only estimates the additional cost of bringing states and territories to the NG911 End State from where they are at Year 0.

The maturity model was developed as a status model, rather than a roadmap, to fully implement NG911 for the entire nation. Hence, not every transitional stage is required in every implementation. The implementation path, identified by SMEs, assumes specific elements that could be skipped during the transitional stages by some of the nation.

While the maturity model includes transitional steps, the costs associated with these transitional steps were merged into the NG911 elements to reduce costs. For example, an IPSR was broken down to basic components of hardware and software, and the geospatial routing element used that same hardware and basic software, then added the additional hardware and software. This was done to reduce the costs, but to also simplify the cost model.

The percentage of progress towards NG911 applied in the cost model is based on the developed NG911 current status. Table D-3 illustrates an aggregated domain level NG911 current status of the NG911 environment. The cost model uses the NG911 functional component current status within a domain at the multistate level to adjust total costs calculated for each element. This is done to estimate the current expected progress of each element within the functional component for each region.

Table D-3: NG911 Domain-level NG911 Current Status

	Legacy	Foundational	Transitional	Intermediate	End State
Business Domain	73.6%	16.4%	2.9%	7.1%	
Data Domain	89.0%		8.2%	2.8%	
Applications and Systems Domain	79.2%	10.0%	1.0%	9.8%	
Infrastructure Domain	88.2%	10.2%		1.6%	
Security Domain	86.9%	7.1%	6.0%		
Operations/ Performance Domain	98.0%	2.0%			

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

D.2.   BUSINESS DOMAIN

The Business Domain consists of those planning and procurement activities that must take place to lay the groundwork for a region's transition to NG911.

Business Domain Assumptions

The cost assumptions and methodologies used in the model are listed later in the section. The cost assumptions and methodologies are listed at the element level and are segmented by cost type. Table D-4 shows those cost types included in the Business Domain at each element level.

Table D-4: Cost Types for Business Domain

Cost Element Structure for Business Domain	Stage	Cost Type				
		Hardware	Software	Services	Staff	Facility
Planning						
Establish NG911 Plan	Foundational			X	X	
Concept of Operations	Transitional			X	X	
Annually Review and Update NG911 Plan	End State			X	X	
Governance						
Gap Analysis	Foundational			X	X	
Governance Plan	Foundational			X	X	
Establish Annually Reviewed Governance	End State			X	X	
Policy						
Gap Analysis	Foundational			X	X	
Establish and Annually Reviewed Policies	Foundational			X	X	
National Governance						
Gap Analysis	Foundational			X	X	
Governance Plan	Foundational			X	X	
Established and Annual Reviewed Governance	End State			X	X	
Procurement						
Procurement Activities throughout Process	Foundational				X	
Implementation						
Statewide Coordination	Foundational				X	
Implementation Project Management	Foundational				X	

Table D-5 shows the total Business Domain costs by cost type for the state implementation and multistate implementation scenarios. Due to the nature of service solution cost calculations, those results are not broken out by the cost type.

Table D-5: NG911 Total Costs for Business Domain by Cost Type

Cost Type	State Implementation Scenario	Multistate Implementation Scenario
Services	$347.2M	$347.2M
Staff	$207.5M	$196.1M
Grand Total	**$554.7M**	**$543.3M**

The predominant cost type associated with functional components of the Business Domain are staff and services costs (labor effort) to perform planning, governance, and procurement activities. Staff costs pertain to government full-time equivalents (FTEs) and service costs pertain to contractor FTEs. Staffing costs do not include normal public safety answering point (PSAP) operations activities, only that which is needed to migrate to NG911. The model uses a domain assumption of factoring labor rates used by a locality factor based on the appropriate region. The model then applies an appropriate regional locality factor. If a region does not have a locality factor, then it will use the "Rest of United States" as a default. (Table D-34 in Section D.8, Reference Tables, shows the localities and their factors.) The FTE level of effort for the Business Domain is identified by subject-matter expert (SME) input. It is scaled by region and is based on a region's ability to coordinate and execute tasks related to emergency communications. This model defines the FTE requirements by levels of strong, medium, and weak for each functional component.

States were grouped into three categories of strong, medium, or weak in the Planning element. This was based on the responses to questions within Section 3.2.1, Planning, of the National 911 Profile Database Survey. States that responded "yes" to question 3.2.1.1, "Has your state developed and adopted a statewide NG911 Plan to include governance, funding, system components (IP network, ESInet, NG911 software services, security architecture, user identity management, database architecture, and PSAP configurations), and operations?" and question 3.2.1.3, "Has your state established a statewide Concept of Operations document, including operations for NG911 and related architecture?" were placed in the strong category. States that responded "yes" to only one of those questions were placed in the medium category. States that responded "no" to all planning questions were placed in the weak category.

Table D-6 indicates the current status of NG911 functional components for the Business Domain at the national level for each NG911 stage from the *2016 National 911 Progress Report*. The total progress is shown as 1-FC NG911 Current Status% within the subsequent cost formulas.

Table D-6: Business Domain NG911 Functional Components Current Status

	Legacy	**Foundational**	**Transitional**	**Intermediate**	**End State**
Planning	42.0%	32.0%		26.0%	
Governance	67.2%	26.7%	0.2%	5.9%	
Policy	96.4%	2.6%	1.0%		
National Governance	100%				
Procurement	61.2%	22.4%	7.1%	9.3%	
Implementation	74.5%	14.6%	9.3%	1.6%	

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

D.2.1. PLANNING

For the majority of states, 911 is operated and managed on a local level, often in siloes and with an independent approach. NG911 is an entirely different concept than what currently exists. More integration and interoperability is needed to improve the effectiveness of NG911 systems. Indeed, statewide coordination is essential for effective NG911 implementation, and operating a statewide 911 system is more complicated than operating a local 911 system. Statewide 911 planning may or may not exist at the Legacy stage. There are two elements of planning, described below.

D.2.1.1.   *Statewide NG911 Plan*

A statewide plan should be created explaining how NG911 will be deployed within the state.[92] The statewide plan is developed in the Foundational stage. The latest recommendations from the Department of Homeland Security (DHS) for the Statewide Communications Interoperability Plan (SCIP) is to include NG911 in the SCIP. In those states without a state authority, it is possible that an NG911 plan may be created at a regional level.

Statewide NG911 Plan Assumptions
This element requires a one-time effort to establish an NG911 plan at the regional level, including government FTEs and contracted services.

- Primary Source(s):
  - SME input, Office of Personnel Management (OPM) labor rates, General Schedule (GS) locality factors, General Services Administration (GSA) Contract Awarded Labor Category (CALC), *2016 National 911 Progress Report*
- Staff Assumption(s):
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.

---

[92] "Draft Report for National 9-1-1 Assessment Guidelines," 911 Resource Center, June 2012, https://resourcecenter.911.gov/911Guidelines/RPT053012_National_911_Assessment_Guidelines_Report_FINAL.pdf.

- o The labor of effort (LOE) used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - o Number FTE staff
    - ▪ Strong – 0.25 FTE
    - ▪ Medium – 0.5 FTE
    - ▪ Weak – 0.5 FTE
  - o Percent of year – 50 percent
- Staff Methodology:
  - o The equation for staffing costs is shown below.
    - ▪ One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - o This element requires one-time service costs for emergency management contractors. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these already are defined as national averages.
  - o The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - o Number FTE staff
    - ▪ Strong – 2 FTEs
    - ▪ Medium – 3 FTEs
    - ▪ Weak – 6 FTEs
  - o Percent of year – 50 percent
- Service Methodology:
  - o The equation for service costs is shown below.
    - ▪ One-time contractor cost = (((annual labor rate of contractor * locality factor) * FTE * duration in % of year * number of region) * (Current Status%))

D.2.1.2.   NG911 Concept of Operations

A detailed concept of operations (ConOps) should be created to guide the transitional process. The ConOps is developed in the Transitional stage and is used through the Intermediate stage.

NG911 Concept of Operations Assumptions
This element requires a one-time government FTE staff and contracted services costs to develop a ConOps for each state within the region.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, GSA CALC, *2016 National 911 Progress Report*, staff assumption(s)
- Staff Assumption(s):
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff
    - Strong – 0.2 FTE
    - Medium – 0.3 FTE
    - Weak – 0.5 FTE
  - Percent of year – 75 percent
- Staff Methodology:
  - The equation for staffing costs is shown below.
    - One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - This element requires one-time services costs for emergency management contractors. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these already are defined as national averages.
  - The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff
    - Strong – 4 FTEs
    - Medium – 5 FTEs
    - Weak – 6 FTEs
  - Percent of year – 75 percent
- Service Methodology:
  - The equation for service costs is shown below.
    - One-time contractor service cost = (((annual labor rate of contractor * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))

D.2.1.3.   Annually Review and Update Statewide NG911 Plan

A statewide plan should be annually reviewed and updated to reflect the current environment.

Annually Review and Update Statewide NG911 Plan Assumptions
This element requires a government FTE staff and contracted services annually to update the statewide NG911 plan.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  - The staff costs for this element are scaled as a percentage (10 percent annual factor) of the total staff costs in the Establish NG911 Plan element.
  - If an area is 100 percent complete with establishing their plan under the Establish NG911 Plan element in the current environment, there are no additional costs for annual review of the plan. This assumes the area already has accounted for this annual update in their current budget.
- Staff Methodology:
  - The equation for staffing costs is shown below.
    - Annual staffing cost = ((total staffing costs * annual staffing cost%) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - The service costs for this element are scaled as a percentage (10 percent annual factor) of the total service costs in the Establish NG911 Plan element.
- Service Methodology:
  - The equation for service costs is shown below.
    - Annual contractor service cost = ((total service costs * annual service cost%) * (1-FC NG911 Current Status%))

D.2.2. GOVERNANCE

For the majority of states, legacy 911 service currently is operated on a local level. To implement NG911 on a regional, tribal, state, or nationwide basis, a governance model needs to be established. Key elements of such an initiative include a gap analysis and a plan.

D.2.2.1.   Governance Gap Analysis

Even those states that have a statewide authority will need to perform a governance gap analysis. It may be necessary to update state statutes prior to moving forward with NG911 planning and transition. The gap analysis is started during the Legacy stage.

Governance Gap Analysis Assumptions

This element requires a government FTE staff and contracted services to analyze the NG911 status and develop a gap analysis at the state level.

- Primary Source(s):
  o SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  o The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  o The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  o Number FTE staff
    ▪ Strong – 0.1 FTE
    ▪ Medium – 0.2 FTE
    ▪ Weak – 0.3 FTE
  o Percent of year – 33 percent
- Staff Methodology:
  o The equation for staffing costs is shown below.
    ▪ One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  o This element requires one-time service costs for emergency management contractors. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these are already defined as national averages.
  o The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  o Number FTE staff
    ▪ Strong – 1 FTE
    ▪ Medium – 1.5 FTEs
    ▪ Weak – 2 FTEs
  o Percent of year – 33.3 percent
- Service Methodology:
  o The equation for service costs is shown below.

- One-time contractor service cost = (((annual labor rate of contractor * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))

D.2.2.2. *Governance Plan*

The state should collaborate with stakeholders to create a comprehensive governance plan for the NG911 system. Even in those areas that have implemented a regional plan and NG911 system, statewide governance is needed to ensure interoperability between regions. The governance plan is developed and implemented in the Foundational through Intermediate stages.

Governance Plan Assumptions
This element requires a one-time effort to establish a governance plan at the regional level, including government FTEs and contracted services.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff
    - Strong – 0.5 FTE
    - Medium – 0.5 FTE
    - Weak – 0.75 FTE
  - Percent of year – 100 percent
- Staff Methodology:
  - The equation for staffing costs is shown below.
    - One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - This element requires one-time service costs for emergency management contractors. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these are already defined as national averages.

- o The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
- o Number FTE staff
  - ▪ Strong – 2 FTEs
  - ▪ Medium – 3 FTEs
  - ▪ Weak – 5 FTEs
- o Percent of year – 100 percent
- • Service Methodology:
  - o The equation for service costs is shown below.
    - ▪ One-time contractor service cost = (((annual labor rate of contractor * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))

D.2.2.3. Annually Review Governance Plan

The governance plan is reviewed and updated on an annual basis to reflect the current environment.

Annually Review Governance Plan Assumptions
This element requires a government FTE staff and contracted services annually to update the governance plan at the regional level.

- • Primary Source(s):
  - o SME input, OPM labor rates, GS locality factors, GSA CALC
- • Staff Assumption(s):
  - o The staff costs for this element are scaled as a percentage (10 percent annual factor) of the total staff costs in the Governance Plan element.
  - o If an area is 100 percent complete with establishing their plan under the Governance Plan element in the current environment, there are no additional costs for annual review of the plan. This assumes the area has already accounted for this annual update in their current budget.
- • Staff Methodology:
  - o The equation for staffing costs is shown below.
    - ▪ Annual staffing cost = ((total staffing costs * annual staffing cost%) * (1-FC NG911 Current Status%))
- • Service Assumption(s):
  - o The service costs for this element are scaled as a percentage (10 percent annual factor) of the total service costs in the Governance Plan element.
- • Service Methodology:
  - o The equation for service costs is shown below.

- Annual contractor service cost = ((total service costs * annual service cost%) * (1-FC NG911 Current Status%))

D.2.3. POLICY

Policies such as security, interconnection, operation, and Identity, Credential, and Access Management (ICAM) at both the PSAP and state levels will need to be updated for the transition to NG911. Key elements of such an initiative include a gap analysis and establishment of policies.

D.2.3.1. Policy Gap Analysis

A gap analysis should be performed to identify those policies that will need to be updated, as well as new policies that may need to be developed. The gap analysis is started in the Legacy stage and continues into the Foundational stage.

There is no information collected in the National Profile Survey related specifically to policy, so the assessment presented is based on SME knowledge of those states that have done either a gap analysis to determine what policies need to be updated or created, or have created updated policies related to NG911. If it was known or documented that a state had conducted a gap analysis and had updated policies for NG911, the state was placed in the strong category. If it was known or documented that a state had conducted a gap analysis, but had not yet effected changes to policies for NG911, the state was placed in the medium category. If no gap analysis had been conducted, the state was placed in the weak category.

Policy Gap Analysis Assumptions
This element requires a one-time effort to develop a gap analysis at the regional level, including government FTEs and contracted services.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  - Staff costs are scaled at the regional level.
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff

- - Strong – 0.1 FTE
    - Medium – 0.2 FTE
    - Weak – 0.3 FTE
  - o Percent of year – 33 percent
- • Staff Methodology:
  - o The equation for staffing costs is shown below.
    - One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))
- • Service Assumption(s):
  - o This element requires one-time service costs for emergency management contractors. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these are already defined as national averages.
  - o The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - o Number FTE staff
    - Strong – 1 FTE
    - Medium – 3 FTEs
    - Weak – 5 FTEs
  - o Percent of year – 33.3 percent
- • Service Methodology:
  - o The equation for service costs is shown below.
    - One-time contractor service cost = (((annual labor rate of contractor * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))

D.2.3.2. Policies

Stakeholders should create and update policies governing NG911. The state may want to provide policy templates for use by PSAPs in updating local policies specifically related to interjurisdictional operations. Policies are created in the Foundational stage and maintained into the End State, where the policies are reviewed and updated on a regular basis.

Policies Assumptions
This element requires a one-time effort to develop policies, as well as an annual effort to update at the regional level, including government FTEs and contracted services.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  - Staff costs are scaled at the regional level.
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff
    - Strong – 0.1 FTE
    - Medium – 0.2 FTE
    - Weak – 0.3 FTE
  - Percent of year – 150 percent
  - The annual staff costs for this element are scaled as a percentage (10 percent annual factor) of the one-time staff costs.
  - If an area is 100 percent complete with establishing their plan under the polices in the current environment, there are no additional costs for annual review of the plan. This assumes the area already has accounted for this annual update in their current budget.
- Staff Methodology:
  - The equations for staffing costs are shown below.
    - One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))
    - Annual staffing cost = ((total staffing costs * annual staffing cost%) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - This element requires one-time service costs for emergency management contractors. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these are already defined as national averages.
  - The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff
    - Strong – 1 FTE
    - Medium – 3 FTEs
    - Weak – 5 FTEs

o   Percent of year – 150 percent
o   The annual service costs for this element are scaled as a percentage (10 percent annual factor) of the one-time service costs.
- Service Methodology:
  o   The equations for service costs are shown below.
    ▪   One-time contractor service cost = (((annual labor rate of contractor * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))
    ▪   Annual contractor service cost = ((total service costs * annual service cost%) * (1-FC NG911 Current Status%))

D.2.4. NATIONAL GOVERNANCE

To facilitate a nationwide transition to NG911, it will be necessary to have some level of national governance. There will be a need for states to interconnect networks to transfer calls, synchronize GIS files, and share data. National governance does not mean a federal agency must operate 911, but there needs to be nationwide coordination by some entity or groups of entities. Key elements of this initiative include a gap analysis and a plan.

D.2.4.1.   *National Governance Gap Analysis*

The gap analysis should identify the areas that require national-level governance to assist in the nationwide transition to NG911. It may be necessary to update statutes prior to moving forward with NG911 planning and transition. The gap analysis is started in the Legacy stage.

States were identified as strong if they had a statewide 911 authority, codified in statute, and could oversee all aspects of the 911 continuum. States were identified as medium if they had some level of authority codified in statute or rules, but only had authority over some portions of the 911 continuum. A state identified as weak had no statewide authority or oversight for NG911.

National Governance Gap Analysis Assumptions
This element requires a one-time effort to develop a national governance gap analysis at the national level, including government FTEs and contracted services.

- Primary Source(s):
  o   SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  o   Staff costs for this element are scaled at the national level.
  o   The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is

factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.

o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.

o Number FTE staff – 0.5 FTE

o Percent of year – 50 percent

- Staff Methodology:
  o The equation for staffing costs is shown below.
    ▪ One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year) * (1-FC NG911 Current Status%))

- Service Assumption(s):
  o This element requires one-time service costs for emergency management contractors. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these are already defined as national averages.
  o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  o Number FTE staff – 6 FTEs
  o Percent of year – 100 percent

- Service Methodology:
  o The equation for service costs is shown below.
    ▪ One-time contractor service cost = (((annual labor rate of contractor * locality factor) * FTE * duration in % of year) * (1-FC NG911 Current Status%))

D.2.4.2. *National Governance Plan*

The national governance plan should identify national stakeholder groups, roles and responsibilities, authority levels, national NG911 system oversight responsibility, and a model for interstate agreements. The national governance plan should be developed and implemented in the Foundational through Intermediate stages. In the End State stage, the national governance plan is reviewed and updated on a regular basis.

National Governance Plan Assumptions
This element requires a one-time effort to develop a national governance plan at the national level, including government FTEs and contracted services.

- Primary Source(s):
  o SME input, OPM labor rates, GS locality factors, GSA CALC

- Staff Assumption(s):
  - o The model assumes that a nationwide coordination authority has been put in place. Therefore, it will not be costed out in this model.
  - o Staff costs for this element are scaled at the national level.
  - o The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - o Number FTE staff – 0.5 FTE
  - o Percent of year – 200 percent
- Staff Methodology:
  - o The equation for staffing costs is shown below.
    - One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - o This element requires one-time service costs for emergency management contractors at the national level. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these are already defined as national averages.
  - o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - o Number FTE staff – 6 FTEs
  - o Percent of year – 200 percent
- Service Methodology:
  - o The equation for service costs is shown below.
    - One-time contractor service cost = (((annual labor rate of contractor * locality factor) * FTE * duration in % of year) * (1-FC NG911 Current Status%))

D.2.4.3.   Regularly Review National Governance Plan

The national governance plan should be reviewed and updated on a regular basis to reflect the current environment.

Regularly Review National Governance Plan Assumptions
This element requires a government FTE staff and contracted services annually to update the national governance plan.

- Primary Source(s):
  - o SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  - o The staff costs for this element are scaled as a percentage (10 percent annual factor) of the total staff costs in the Governance Plan element.
- Staff Methodology:
  - o The equation for staffing costs is shown below.
    - Annual staffing cost = ((total staffing costs * annual staffing cost%) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - o The service costs for this element are scaled as a percentage (10 percent annual factor) of the total service costs in the Governance Plan element.
- Service Methodology:
  - o The equation for service costs is shown below.
    - Annual contractor service cost = ((total service costs * annual service cost%) * (1-FC NG911 Current Status%))

D.2.5. PROCUREMENT

The procurement of NG911 equipment, components, and services will be ongoing throughout the transition to NG911. Procurement will include an ESInet, 911 call-handling equipment, recording and logging equipment, GIS and mapping services, NGCS, and possibly multiple levels of system management services.

Procurement Assumptions
This element requires government FTE staff annually at the regional level to oversee all aspects of the NG911 procurement process.

- Primary Source(s):
  - o SME input
- Staff Assumption(s):
  - o The staff costs for this element are calculated as 1 percent (industry factor for acquisition processes) of the total NG911 investment and operation activities (i.e., the cost of any request for proposals [RFP] documentation, specifications, evaluations, contract negotiations, and other necessary bidding processes).

D.2.6. IMPLEMENTATION

Implementation of NG911 equipment, components, and services will be ongoing throughout the transition to NG911. Implementation will include an ESInet, 911 call-handling equipment,

recording and logging equipment, GIS and mapping services, NGCS, and possibly multiple levels of system management services.

D.2.6.1.   *Statewide Implementation Coordination*

This element provides for state-level oversight of the implementation of NG911 equipment, components, and services. A systems integrator, statewide coordination, and monitoring of implementation costs are included in this element.

Statewide Implementation Coordination Assumptions
This element requires a one-time government FTE staff for systems integration, as well as statewide coordination and monitoring of implementation. These costs are scaled at the regional level.

- Primary Source(s):
    - SME input, OPM labor rates, GS locality factors
- Staff Assumption(s):
    - Other implementation costs (e.g., hardware, software, etc.) are included within the appropriate domains. Therefore, they will not be costed out in this element.
    - Staff costs for this element are scaled at the regional level.
    - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
    - The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
    - Number FTE staff – 1 FTE
    - Percent of year – 100 percent
- Staff Methodology:
    - The equation for staffing costs is shown below.
        - One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))

D.2.6.2.   *Implementation Project Management*

Technical project management will be required for implementation of NG911 equipment, components, and services. This project management may come from within state staff, or may need to be contracted from a third party.

Implementation Project Management Assumptions

This element requires a one-time effort to implement project management for NG911 activities at the regional level, including government FTEs.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors
- Staff Assumption(s):
  - Staff costs for this element are scaled at the regional level.
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff – 2 FTEs
  - Percent of year – 100 percent
- Staff Methodology:
  - The equation for staffing costs is shown below.
    - Annual staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of region) * (1-FC NG911 Current Status%))

D.3. DATA DOMAIN

The Data Domain captures the data management responsibilities of PSAPs, regions, tribes, states, and national-level authorities as they prepare for and implement NG911. This domain includes a shift from tabular location data to full dependency on GIS data for the verification of caller location and routing of 911 calls, as well as managing information in additional data repositories.

Data Domain Assumptions

The cost assumptions and methodologies used in the model are listed later in this section. The cost assumptions and methodologies are listed at the element level and segmented by cost type. Table D-7 shows those cost types included in the Data Domain at each element level. Costs include hardware, services, staff, and software.

Table D-7: Cost Types for Data Domain

Cost Element Structure for Data Domain	Stage	Cost Type				
		Hardware	Software	Services	Staff	Facility
Geospatial Information Systems Data						
Developing Regional and Statewide Datasets	Foundational	x	x	x	x	
Maintain Statewide Datasets	Intermediate			x	x	
Location Data						
Location Database (LDB)	Intermediate			x		

Table D-8 indicates the total Data Domain costs by cost type for the state implementation and multistate implementation scenarios. Due to the nature of service solution cost calculations, those results are not broken out by the cost type.

Table D-8: NG911 Total Costs for Data Domain by Cost Type

Cost Type	State Implementation Scenario	Multistate Implementation Scenario
Hardware	$2.4M	$1.1M
Services	$533.7M	$426.4M
Staff	$1,067.7M	$1,067.7M
Software	$86.1M	$86.1M
Grand Total	**$1,689.9M**	**$1,581.3M**

Table D-9 indicates the current status of NG911 functional components for the Data Domain at the national level. The total progress is shown as 1-FC NG911 Current Status% within the subsequent cost formulas.

Table D-9: Data Domain NG911 Functional Components Current Status

	Legacy	Foundational	Transitional	Intermediate	End State
Geographic Information System	67.3%		32.7%		
Location Data	88.9%			11.1%	
Additional Data	100%				
System Control and Management	100%				

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

D.3.1. GEOGRAPHIC INFORMATION SYSTEMS DATA

GIS data represents local, regional, state, federal, and tribal jurisdictions, as well as location information, through a set of lines, polygons, and attributes. GIS data is layered to provide multiple sets of information for a single latitude-and-longitude location.

D.3.1.1. Local or No Data

GIS data is not available or is locally managed, with little to no maintenance of the dataset. GIS data has little to no correlation to automatic location identification (ALI) and Master Street Address Guide (MSAG) data at the Legacy stage.

Local or No Data Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.3.1.2. Developing Regional and Statewide Datasets

GIS data is being compared with MSAG and ALI datasets.[93] Regional and statewide data models are being developed for eventual use in validating caller location and call routing. Regional and statewide data is developed in the Foundational and Transitional stages.

Developing Regional and Statewide Data Sets Assumptions
This element requires a one-time government FTE staff effort at the regional level and county level to develop and coordinate datasets at the regional level. This element also requires GIS database servers and GIS software licenses at the regional level. Services for maintaining datasets at the regional level also are required.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, GSA CALC, U.S. Census, vendor pricing, GSA Advantage pricing, NG911 publicly available cost studies
- Staff Assumption(s):
  - Staff costs for this element are scaled at the regional and county level.

---

[93] "Synchronizing GIS with MSAG & ALI," National Emergency Number Association, September 8, 2009, https://www.nena.org/?page=synch_gis_msag_ali.

- o The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
- o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
- o Number FTE Staff
  - ▪ Per region – 0.5 FTE
  - ▪ Per county – 1 FTE
- o Percent of year
  - ▪ Per region – 100 percent
  - ▪ Per county – 100 percent

- • Staff Methodology:
  - o The equations for staffing costs are shown below.
    - ▪ Regional level staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of state) * (1-FC NG911 Current Status%))
    - ▪ County level staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of counties) * (1-FC NG911 Current Status%))

- • Hardware Assumption(s):
  - o The quantity of servers is scaled by the size and quantity of cores per region. This includes redundancy and one-time procurement costs, recurring maintenance costs, and refresh costs.

- • Hardware Methodology:
  - o The equations for hardware costs are shown below.
    - ▪ One-time server procurement cost = ((quantity of core * number of servers * unit cost) * (1-FC NG911 Current Status%))
    - ▪ Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - ▪ Refresh cost = (total procurement cost + installation cost)

- • Software Assumption(s):
  - o There are GIS enterprise software licensing fees at the regionwide level. This will include the development of customized software for quality assurance and quality control (QA/QC).

- • Software Methodology:
  - o The equation for software costs is shown below
    - ▪ Annual GIS software = ((software annual fee * number of counties) * (1-FC NG911 Current Status%)) + ((industry GIS software enterprise annual fee * number of states) * (1-FC NG911 Current Status%))

- Service Assumption(s):
  - o The service costs are based on size of the datasets, which are scaled by the population. For this cost study, populations that define the GIS service fees are categorized into three levels based on SME input.
    - ▪ Population level 1: up to 500,000 population served – $500,000 annual GIS service cost
    - ▪ Population level 2: up to 5,000,000 population served – $4,000,000 annual GIS service cost
    - ▪ Population level 3: up to 10,000,000 population served – $7,000,000 annual GIS service cost
- Service Methodology:
  - o The equations for service costs are shown below.
    - ▪ GIS data management and maintenance cost = ((vendor fee in units * region population * number of states) * (1-FC NG911 Current Status%))
    - ▪ Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.3.1.3. GIS for Location Verification

GIS, ALI, and MSAG datasets are manipulated to enhance match rates. Data maintenance processes are developed and maintained. GIS data management processes may be at a stage that provides for caller location data to be verified to GIS data, as opposed to the traditional tabular MSAG data. Location validation is performed starting in the Transitional stage through the End State stage.

GIS for Location Verification Assumptions
Current staff will need to maintain datasets and support data verification activities; therefore, from a cost perspective, there is no additional cost for NG911. Similar to the current environment, vendors will manage ALI data sets daily.

D.3.1.4. Maintain Developed Statewide Dataset

GIS data has 98 percent or greater match rate with the MSAG and ALI datasets.[94] Regional datasets, including all required boundary layers, have been coalesced into a congruent statewide dataset. GIS data is in the maintenance phase. A statewide data model is developed and available for use in validating caller location and call routing. Statewide data is established in the Intermediate stage.

---

[94] Ibid.

Maintain Developed Statewide Dataset Assumptions

This element requires a government FTE staff effort and vendor services to maintain and manage datasets. FTE staff efforts are needed at the regional level and county level, while vendor services are needed only at the core level.

- Primary Source(s):
  o SME input, OPM labor rates, GS locality factors, U.S. Census, vendor pricing, GSA Advantage pricing, NG911 publicly available cost studies
- Staffing Assumption(s):
  o Maintaining statewide datasets is captured in the ongoing staffing of *Developing Regional and Statewide Datasets* element.
  o Once NG911 services are initiated, there will be FTE staffing costs at the regional level and at the county level.
  o It is assumed that the maintenance of datasets and validations will be performed by government staff instead of by contract services.
  o The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  o Number FTE staff
    - Per region – 1.5 FTEs
    - Per county – 0.25 FTE
  o Percent of year
    - Per region – 100 percent
    - Per county – 100 percent
- Staffing Methodology:
  o The equations for staffing costs are shown below.
    - Regional level staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of state) * (1-FC NG911 Current Status%))
    - County level staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of counties) * (1-FC NG911 Current Status%))
- Software Assumption(s):
  o Software costs for this element are captured and maintained in the *Developing Regional and Statewide Datasets* element. Therefore, they are not costed out in this element.
- Service Assumption(s):
  o Service costs are scaled by the population.

- Service Methodology:
  - The equation for service costs is shown below
    - GIS data maintenance cost = ((vendor fee in units * regional population * number of state) * (1-FC NG911 Current Status%))

D.3.1.5.   GIS for Routing

GIS data and data maintenance processes have matured to the point that the dataset may be used for live 911 call routing. GIS data is now used for all location-validation purposes. GIS routing is performed starting in the Intermediate stage through the End State stage.

GIS for Routing Assumptions
Related costs are captured in the Geospatial Routing with Traditional Rules element within the Applications and Systems Domain. Therefore, they are not costed out in this element

D.3.1.6.   National GIS Dataset

Statewide GIS datasets are coordinated with neighboring states to provide for a seamless national data set. GIS data is solely used for location validation and call routing. Nationwide datasets are available in the End State stage.

National GIS Dataset Assumptions
At the time of this estimate, there is no clear authority that coordinates statewide datasets for a seamless national dataset. This cost study is not able to clearly define a cost for this element due to political factors and lack of agency authority. Costs of this element will be recovered via the normal federal budgeting process.

D.3.2. LOCATION DATA

Location data involves the information and systems used to provide PSAPs and first responders with information regarding where an emergency may be found.

D.3.2.1.   Traditional ALI

Traditional ALI data is maintained for wireline and voice over IP (VoIP) callers. Wireless cellular tower address information is maintained in supplemental databases and queried for Phase I and Phase II location information. Traditional data is used from the Legacy stage through the Transitional stage. In the Legacy stage, location data is delivered over dedicated, point-to-point ALI circuits. In the Foundational stage, location data may now be delivered to PSAPs over an IP

network, if such a network is in place. In the Transitional stage, location data may now be delivered to PSAPs over an IP network through a traditional ALI bid.

Traditional ALI Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.3.2.2. Location Database (LDB)

The LDB maintains traditional ALI data in conjunction with additional caller information. NG911 standards-based interfaces are used to retrieve location information at varying stages of call setup to enable an NG911 call flow.[95] The LDB is used in the Intermediate stage.

LDB Assumptions

- Primary Source(s):
  - SME input, vendor pricing, NG911 publicly available cost studies
- Service Assumption(s):
  - Service costs for this element include the management of the LDB for the state. This is derived from the size of the core, which was based on the population served for each core.
- Service Methodology:
  - The equation for service costs is shown below.
    - LDB management = ((vendor unit cost from core size * number of cores) * (1-FC NG911 Current Status%))

D.3.2.3. Location Information Server (LIS)

Location data is provided by an LIS using NG911 interfaces and protocols. The LIS is used in the End State stage.[96]

This is a continuation of what is initiated within the LDB. There are no additional costs for this data.

---

[95] "NG9-1-1 Transition Planning Considerations," National Emergency Number Association, November 20, 2013, http://www.nena.org/?page=NG911_TransitionPlng.
[96] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, http://www.nena.org/?page=i3_Stage3.

D.3.3. ADDITIONAL DATA

Additional information regarding a call, caller, or location may be available to a call-taker and/or first responder to enhance situational awareness and improve emergency response.[97]

D.3.3.1.   Silo and Proprietary Data

Additional data may be available through disparate and proprietary systems offering little to no interoperability between PSAP 911 systems, such as call handling and computer-aided dispatch (CAD), within a PSAP and with other PSAPs. Examples of additional data in this stage include Advanced Automated Collision Notification (AACN) and personal safety applications with proprietary and/or Web-based interfaces. Silo systems exist from the Legacy stage through the Transitional stage.

Silo and Proprietary Data Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.3.3.2.   Shared Standards-based Data

Additional data may be accessed through standards-based interfaces and shared across multiple NG911 systems. PSAPs across a region or state may be able to access the same data where network connectivity and authorization is established. The examples of AACN and personal safety applications migrate from proprietary interfaces with limited access to standards-based data structures, such as Extensible Markup Language (XML), accessed by standards-based data-retrieval interfaces, such as Hypertext Transfer Protocol (HTTP) GET, and secured by standards-based protocols such as Transport Layer Security (TLS). Standards-based systems are implemented in the Intermediate stage through the End State stage.

Shared Standards-based Data Assumptions
While this element requires service costs, there are no costs included in this study as this represents new unknown service costs.

D.3.4. SYSTEM CONTROL AND MANAGEMENT DATA

This refers to data related to the day-to-day control and management of NGCS. This data typically includes, but is not limited to, internal network element log files, network bandwidth utilization data, Simple Network Management Protocol (SNMP) traps, server operating system log files, data storage utilization, system access and session logs, failed login attempts, and password resets.

---

[97] "NG9-1-1 Additional Data," National Emergency Number Association, September 17, 2009, https://www.nena.org/?page=NG911_AdditionalData.

D.3.4.1.   Silo and Proprietary Data

The various systems operate in silos and do not share data or information.

Silo and Proprietary Data Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.3.4.2.   Shared Standards-based Data

The various systems share data and information to include Event Logging and Policy Routing Function (PRF) data.

Event Logging data includes, but is not limited to, the time the call entered the network, which core components handled the routing, when the call was passed from one component to another, and whether the call was placed on hold, transferred, or conferenced with other agencies.

PRF data is data describing the call-routing rules that agencies implement in the PRF functional element.

Shared Standards-based Data Assumptions
While this element requires service costs, there are no costs included in this study as this represents new unknown service costs.

D.4.   APPLICATIONS AND SYSTEMS DOMAIN

The Applications and Systems Domain describes the applications, systems and other core functions of the NG911 systems.

Applications and Systems Domain Assumptions
The cost assumptions and methodologies used in the model are listed later in this section. The cost assumptions and methodologies are listed at the element level and are segmented by cost type. Table D-10 shows those cost types included in the Applications and Systems Domain at each element level. Costs include services, hardware, and software.

Table D-10: Cost Types for Applications and Systems Domain

Cost Element Structure for Application and Systems Domain	Stage	Cost Type				
		Hardware	Software	Services	Staff	Facility
Call Routing						
IP Selective Routing	Foundational	x	x	x		
Geospatial Routing with Traditional Rules	Intermediate	x		x		
Geospatial Routing with Progressive Rules	End State	x	x	x		
Call Handling						
IP-based Call Handling System	Intermediate	x		x		
Location Validation						
Geospatial Validation	Intermediate	x	x	x		
Location Delivery						
Delivery by PIDF-LO in SIP header	Intermediate			x		
Call Processing						
Standards-based systems	Intermediate		x			
Event Logging						
End-to-end Integrated Logging	Intermediate	x	x	x		
Data Analysis						
Automated Data Analytics in Place	Intermediate	x	x	x		
Forest Guide						
Forest Guide in Place	Intermediate	x		x		
National Forest Guide	End State	x		x		

Table D-11 shows the total Applications and Systems Domain costs by cost type for the state implementation and multistate implementation scenarios. Due to the nature of service solution cost calculations, those results are not broken out by the cost type.

Table D-11: NG911 Total Costs for Applications and Systems Domain by Cost Type

Cost Type	State Implementation Scenario	Multistate Implementation Scenario
Hardware	$1,654.6M	$1,641.7M
Services	$4,736.6M	$4,733.9M
Software	$1,372.5M	$1,085.0M
Grand Total	**$7,763.7M**	**$7,460.7M[98]**

Table D-12 indicates the current status of the NG911 functional components for the Applications and Systems Domain at the national level. The total progress is shown as 1-FC NG911 Current Status% within the subsequent cost formulas.

---

[98] Please note that these figures are rounded in the millions for simplicity. Thus, these figures do not add to the grand total due to the rounding factor, but align with the tables in Appendix E, Cost Analysis Detailed Results.

Table D-12: Applications and Systems Domain NG911 Functional Components Current Status

	Legacy	**Foundational**	**Transitional**	**Intermediate**	**End State**
Call Routing	87.0%	10.0%		3.0%	
Call Handling Systems	45.0%			55.0%	
Location Validation	85.1%			14.9%	
Location Delivery	17.1%	69.7%	8.0%	5.2%	
Call Processing	100%				
Event Logging	100%				
Data Analytics	100%				
Forest Guide	100%				

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

D.4.1. CALL ROUTING

Call-routing applications evaluate data contained in the call to determine the proper PSAP to receive that call. The existing Enhanced 911 (E911) systems use address data in tabular files to determine proper call routing. As 911 transitions to NG911, routing decisions will be based on geographic data contained in databases. In some cases, a 911 authority may move from the Legacy stage to the Intermediate stage without implementing the Foundational or Transitional stages.

D.4.1.1. Trunk or Selective Routing

Routing is accomplished primarily through selective routing in tandem switches of communication service providers (CSPs). In some cases, direct trunks are used between the CSP and PSAP. In either case, routing is based on tabular data files containing address and emergency service number (ESN) information. The ESN is mapped to a particular PSAP. Trunk or selective routing is performed in the Legacy stage.

Trunk or Selective Routing Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.4.1.2. IP Selective Routing

IP selective routing begins to replace circuit-switched legacy selective routing as calls are converted from Time Division Multiplexing (TDM) to VoIP. Routing information remains in a tabular file format. IP selective routing is performed in the Foundational stage and continues into the Transitional stage.

IP Selective Routing Assumptions

This element requires IP routers at the PSAP and at the core level. Load balancers, application servers, and database servers are required at the core level. This element requires Emergency Services Routing Proxy (ESRP) software costs to perform the NG911 Specific Interwork Function (NIF), Location Interwork Function (LIF), and Protocol Interworking Function (PIF).

- Primary Source(s):
  - SME input, U.S. Census, *2016 National 911 Progress Report*, *Voice Telephone Services* report (2015), *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, vendor pricing, GSA Advantage pricing, NG911 publicly available cost studies
- Hardware Assumption(s):
  - The hardware costs include one-time procurement costs, recurring maintenance costs, and refresh costs.
  - The size of the IP router at the PSAP level is scaled based on the PSAP size. PSAP sizes are defined by the number of positions. For this cost study, they are grouped into four categories: small, medium, large, and mega.
  - At the core level, the router size is scaled to the size of the core for that area, which is defined by SMEs. For this cost study, cores are grouped into three categories: small, medium, and large.
  - Load balancers, application servers, and database servers require redundancy at the core level.
- Hardware Methodology:
  - The equations for hardware costs are shown below.
    - One-time PSAP router procurement cost = ((quantity of small PSAPs * number of routers * unit cost) + (quantity of medium PSAPs * number of routers * unit cost) + (quantity of large PSAPs * number of routers * unit cost) + (quantity of mega PSAPs * number of routers * unit cost) * (1-FC NG911 Current Status%))
    - One-time core hardware procurement cost = ((quantity of core * number of hardware * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M hardware cost = ((total hardware procurement cost * O&M%) * (1-FC NG911 Current Status%))

- Refresh hardware cost = (total hardware procurement cost + hardware installation cost)
- Software Assumption(s):
  - These costs are for software purchasing and licensing costs that are scaled by the number of cores in an area. These costs include an annual licensing fee as well as an annual maintenance cost.
- Software Methodology:
  - The equations for software costs are shown below.
    - Annual software and licensing cost = ((quantity of cores * software license) * (1-FC NG911 Current Status%))
    - Software maintenance cost = ((total annual software cost * software maintenance cost%) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - Service costs for hardware installation are based at the core and PSAP level.
- Service Methodology:
  - The equation for the service costs are shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.4.1.3. *Geospatial Routing with Traditional Rules*

Geospatial routing databases replace the tabular files used in call routing. Traditional rules-based routing, such as alternate and default routing, is implemented in the routing systems. Geospatial routing with traditional rules resides in the Intermediate stage.

Geospatial Routing with Traditional Rules Assumptions
This element requires additional application servers for the Emergency Call Routing Function (ECRF) at each core, as well as software updates for the ECRF at each PSAP.

- Primary Source(s):
  - SME input, U.S. Census, *2016 National 911 Progress Report, Voice Telephone Services* report (2015), *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, vendor pricing, GSA Advantage pricing, NG911 publicly available cost studies
- Hardware Assumption(s):
  - This element uses the hardware listed in the IP Selective Routing element and, therefore, will not be costed out in this element.
  - Hardware costs include one-time procurement costs, recurring maintenance costs, and refresh costs. The application servers are scaled by core size. Each core will require two servers for redundancy.

- Hardware Methodology:
  - The equations for hardware costs are shown in Table D-13 below.
    - One-time server procurement cost = ((quantity of core * number of servers * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - Refresh cost = (total procurement cost + installation cost)
- Software Assumption(s):
  - This element will use the software listed in the *IP Selective Routing* element and, therefore, will not be costed out in this element.
  - These costs include one-time software update procurement costs and recurring operational costs. This cost is scaled based on the number of PSAPs per area.

Table D-13: Annual ECRF Operational Costs (Provided by SME)

Core Size	Annual ECRF Service Costs
Small	$175,000
Medium	$250,000
Large	$500,000

- Software Methodology:
  - The equations for software costs are shown below.
    - One-time software procurement update = ((number of PSAPs * unit cost) * (1-FC NG911 Current Status%))
    - Annual software operations cost = ((number of PSAPs * annual unit cost) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - This element requires service costs for hardware installation.
- Service Methodology:
  - The equation for hardware costs is shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.4.1.4. *Geospatial Routing with Progressive Rules*

All NGCS are fully functional and all calls are routed based on geospatial data and a progressive set of configurable rules under the control of the PSAPs and 911 authorities. Geospatial and progressive rules-based routing is performed in the End State stage.[99]

---

[99] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, http://www.nena.org/?page=i3_Stage3.

Geospatial Routing with Progressive Rules Assumptions

This element requires hardware modifications for the application and database servers installed in the IP Selective Routing and Geospatial Routing with Traditional Rules elements. This element also requires modifications for the ESRP and ECRF software defined in the IP Selective Routing and Geospatial Routing with Traditional Rules elements.

- Primary Source(s):
  - SME input, U.S. Census, *2016 National 911 Progress Report*, *Voice Telephone Services* report (2015), *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, vendor pricing, GSA Advantage pricing, NG911 publicly available cost studies
- Hardware Assumption(s):
  - The hardware modification cost is a one-time cost based on the percentage of total costs of the application servers.
- Hardware Methodology:
  - The equation for hardware costs is shown below.
    - Hardware modification cost = ((total hardware procurement cost * hardware modification%) * (1-FC NG911 Current Status%))
- Software Assumption(s):
  - The software modification cost is a one-time cost based on the percentage of total costs of the application software licensing.
- Software Methodology:
  - The equation for software costs is shown below.
    - One-time software modification cost = ((total ESRP software procurement cost + total ECRF software procurement cost) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - This element requires service costs for the installation of the hardware.
- Service Methodology:
  - The equation for service costs is shown below.
    - Installation cost = ((total software modification cost * installation%) * (1-FC NG911 Current Status%))

D.4.2. CALL HANDLING SYSTEMS

Call-handling systems connect the call to a telecommunicator, who then gathers the information from the caller and relays that information to responding agencies. Legacy call-handling systems are referred to as customer premises equipment (CPE); they handle only voice calls and receive those calls via analog trunks. IP-capable systems accept calls from direct Session Initiation Protocol (SIP) connections and, with the proper software, may accept multiple call types.

D.4.2.1. Legacy CPE

Equipment is capable only of processing voice calls. Primarily an analog 911 system, some later releases of CPE software may support early implementations of SIP call delivery, such as Request for Assistance Interface (RFAI). A legacy PSAP gateway (LPG) is required to connect CPE to an ESInet for SIP call delivery. Legacy CPE will exist through the Transitional stage.

Legacy CPE Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.4.2.2. IP-based Call Handling Systems

IP-based systems are capable of direct SIP delivery of calls, and may accept any valid SIP call type that may be implemented in the application software. As new call types are developed, the call-handling system can be upgraded through software releases to accept and process the new call types. IP-based call-handling systems will appear in the Intermediate stage and continue through the End State stage.

IP-based Call Handling Systems Assumptions
This element requires workstation software and equipment for each PSAP position.

- Primary Source(s):
  - SME input, U.S. Census, *2016 National 911 Progress Report*, *Voice Telephone Services* report (2015), *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, vendor pricing, GSA Advantage pricing, NG911 publicly available cost studies
- Hardware Assumption(s):
  - Hardware costs include one-time procurement costs, recurring maintenance costs, and refresh costs. Costs are scaled based on the number of PSAP positions. Mega PSAP workstations have lower costs due to economies of scale. A summary of these costs is shown in Table D-14.

Table D-14: Workstation Costs

PSAP Size	Workstation Cost
Small	$42,281
Medium	$42,281
Large	$42,281
Mega	$22,414

- Hardware Methodology:
  - o The equations for hardware costs are shown below.
    - ▪ One-time workstation procurement cost = (((quantity of PSAP * quantity of PSAP positions) * unit cost) * (1-FC NG911 Current Status%))
    - ▪ Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - ▪ Refresh cost = (total procurement cost + installation cost)
- Software Assumption(s):
  - o Software costs are scaled based on the number of PSAP positions.
- Software Methodology:
  - o The equation for software costs is shown below.
    - ▪ Annual workstation software cost = ((number of PSAPs * annual unit cost) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - o This element requires service costs for hardware installation.
- Service Methodology:
  - o The equation for service costs is shown below.
    - ▪ Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.4.3. LOCATION VALIDATION

Location validation checks the address against an authoritative dataset to verify the validity of the call location. The dataset is a tabular file in the legacy environment and a true relational database in the NG911 environment. In some cases, a 911 authority may move from the Legacy stage to the Intermediate stage without implementing the Foundational or Transitional stages.

D.4.3.1. MSAG Validation

Location validation is performed using an MSAG tabular file. MSAG validation is performed in the Legacy stage and continues through the Transitional stage.

MSAG Validation Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.4.3.2. Geospatial Validation

Geospatial validation is implemented to validate the location data from the communications service provider (CSP). Geospatial validation is performed from the Intermediate stage through the End State stage.[100]

Geospatial Validation Assumptions

This element requires Web servers and Location Validation Function (LVF) software at each core to replicate the geospatial database for verification.

- Primary Source(s):
  - SME input, U.S. Census, *2016 National 911 Progress Report*, *Voice Telephone Services* report (2015), *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, vendor pricing, GSA Advantage pricing, NG911 publicly available cost studies
- Hardware Assumption(s):
  - Hardware costs include one-time procurement costs, recurring maintenance costs, and refresh costs. Cost is scaled by core size and includes a hardware redundancy factor.
- Hardware Methodology:
  - The equations for hardware costs are shown below.
    - One-time web server procurement cost = ((quantity of core * number of servers * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - Refresh cost = (total procurement cost + installation cost)
- Software Assumption(s):
  - Software costs are based on core size and include one-time software procurement costs and annual software operations costs, as shown in Table D-15.

---

[100] "NG9-1-1 Transition Planning Considerations," National Emergency Number Association, November 20, 2013, http://www.nena.org/?page=NG911_TransitionPlng.

Table D-15: Software Costs (Provided by SME)

Core Size	Non-recurring Costs	Annual Recurring Costs
Small	$49,000	$8,400
Medium	$70,000	$12,000
Large	$140,000	$24,000

- Software Methodology:
  - The equations for software costs are shown below.
    - One-time software procurement cost = ((number of cores * unit cost) * (1-FC NG911 Current Status%))
    - Annual software cost = ((number of cores * unit cost) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - This element requires service costs for hardware installation.
- Service Methodology:
  - The equation for service costs is shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.4.4. LOCATION DELIVERY

The location of a caller is provided to the PSAP to enable the dispatching of emergency services to the accurate location. Location delivery will move from a database bid after call delivery in a legacy environment to being delivered with the call in the Intermediate and End State stages. In some cases, a 911 authority may move from the Legacy stage to the Intermediate stage without implementing the Foundational or Transitional stages.

D.4.4.1. *Post Call Delivery over Dedicated ALI Circuits*

The PSAP must query a database over serial data circuits and receive a response to obtain the ALI information after the call is received at the PSAP. Post call delivery over dedicated ALI circuits is performed in the Legacy stage.

Post Call Delivery over Dedicated ALI Circuits Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.4.4.2.   Post Call Delivery over Dedicated IP Circuits

The delivery of legacy ALI data and NG911 location data will continue as PSAPs transition to NG911. The implementation of IP-based delivery methods over dedicated IP circuits will reduce circuit costs. Delivery over IP exists in the Foundational stage.

Post Call Delivery over Dedicated IP Circuits Assumptions
Related costs are captured in the LDB element within the Applications and Systems Domain. Therefore, it is not costed out in this element. The costs associated with this are captured in other elements, but this may permit the retiring of legacy ALI data circuits early.

D.4.4.3.   Delivery over IP Circuits

The delivery of legacy ALI data and NG911 location data will continue as PSAPs transition to NG911. The implementation of IP-based delivery methods over the ESInet will reduce circuit costs. Delivery over IP exists in the Transitional stage.

Delivery over IP Circuits Assumptions
Related costs are captured in the LDB element within the Applications and Systems Domain. Therefore, it is not costed out in this element.

D.4.4.4.   Delivery by PIDF-LO in SIP Header

NG911 location information is encapsulated in the Presence Information Data Format – Location Object (PIDF-LO) and included in the SIP header as part of the call setup. PIDF-LO is used in the Intermediate and End State stages.[101]

Delivery by PIDF-LO in SIP Header Assumptions

- Primary Source(s):
  - SME input, *Voice Telephone Services* report (2015), *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, vendor pricing
- Service Assumption(s):
  - This element requires service costs and is scaled based on the number of service providers within an area.

---

[101] "NENA i3 Solution – Stage 3," National Emergency Number Association, September 10, 2016, http://www.nena.org/?page=i3_Stage3.

- o The costs associated with this element are applied to the CSP or originating service provider (OSP), such as legacy phone-provider companies.
- Service Methodology:
  - o The equation for service costs is shown below.
    - Annual service cost = ((number of switches * service unit cost) * (1-FC NG911 Current Status%))

D.4.5. CALL PROCESSING

Call-processing equipment processes the information from the call and delivers it to the responders in the field. Call-processing equipment includes CAD systems and mobile data systems.

D.4.5.1.   Silo and Proprietary Systems

Call-processing equipment has proprietary systems and interconnections. These systems will exist from the Legacy stage through the Transitional stage.

Silo and Proprietary Systems Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.4.5.2.   Standards-based Systems

The systems use open standards that permit data sharing between diverse NG911 systems. Standards-based systems will appear in the Intermediate stage and continue through the End State stage.

Standards-based Systems Assumptions

- Primary Source(s):
  - o SME input, *2016 National 911 Progress Report*, vendor pricing
- Software Assumption(s):
  - o This element requires CAD software licensing costs. This cost is scaled at the PSAP level and is based on the number PSAP positions.
- Software Methodology:
  - o The equation for software costs is shown below.
    - Annual software and licensing cost = ((number of PSAPs * annual unit cost) * (1-FC NG911 Current Status%))

D.4.6. EVENT LOGGING

Event logging is the capture and storage of all information related to a given call. This includes, but is not limited to, the time the call entered the network, which core components handled the routing, when the call was passed from one component to another, the media (voice, video, photo, text) of the call, and whether the call was placed on hold, transferred, or conferenced with other agencies. It is a complete record of how the call was handled.[102]

D.4.6.1.   Silo and Proprietary Data in Separate Systems

Each disparate system maintains its own logging of events, creating silos of information. Compilation of data between systems and various system operators to form a complete picture can be tedious. Silo and proprietary systems are in place from the Legacy stage to the Transitional stage.

Silo and Proprietary Data in Separate Systems Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.4.6.2.   End-to-end Integrated Logging

The logging of information is consolidated, reported to, or accessible from a system that can compile all information for a single call into a single log for troubleshooting or monitoring. End-to-end logging is implemented in the Intermediate stage and continues into the End State stage.

End-to-end Integrated Logging Assumptions
This element requires servers to store and archive large amounts of data for the end-to-end integrated logging functionality. This element requires software for customized databases to conduct comprehensive data searches. Both are needed at the regional level.

- Primary Source(s):
  - SME input, U.S. Census, *2016 National 911 Progress Report*, vendor pricing
- Hardware Assumption(s):
  - The hardware costs are scaled based on the population of each area and include one-time procurement costs, recurring maintenance costs, and refresh costs.
- Hardware Methodology:
  - The equations for hardware costs are shown below.
    - One-time server procurement cost = ((region population * unit cost) * (1-FC NG911 Current Status%))

---

[102] Ibid.

- - Annual O&M cost = ((region population * O&M unit cost) * (1-FC NG911 Current Status%))
    - Refresh cost = (total procurement cost + installation cost)
  - Software Assumption(s):
    o Software costs are scaled based on the population of each area. These costs include one-time procurement costs and recurring maintenance costs.
  - Software Methodology:
    o The equations for software costs are shown below.
      - One-time software procurement cost = ((region population * unit cost) * (1-FC NG911 Current Status%))
      - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
  - Service Assumption(s):
    o This element requires service costs for hardware installation.
    o The element also requires service costs for event logging.
  - Service Methodology:
    o The equations for service costs are shown below.
      - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))
      - Annual service cost = ((region population * service unit cost) * (1-FC NG911 Current Status%))

D.4.7. DATA ANALYTICS

Data analytics currently present a challenge because of the proprietary and siloed nature of the components comprising the present 911 system. NG911 may bring a large amount of data to the public safety system. The NG911 system's ability to get the right data to the right people at the right time will enhance emergency response. Data analytics provide a means for the NG911 system to process large amounts of data based on the needs of the system participants. Data analytics also refer to the statistical processing of data collected in the event logging systems to detect trends, anomalies, and, potentially, problems.

D.4.7.1.   Automated Data Analytics

The users, governing body, state, or 911 authorities will develop or adopt standards and procedures for data analytics. With standards-based logging and additional data sources implemented in all NG911 systems, data can be analyzed to reduce the information presented to the PSAP or passed directly to responders, to make better routing decisions and to provide better service to the public. Automated data analytics begins in the Intermediate stage and continues into the End State stage.

Automated Data Analytics Assumptions

This element requires core level application servers and software for data analytics and performance functionalities.

- Primary Source(s):
  - o SME input, *2016 National 911 Progress Report*, *Voice Telephone Services* report (2015), *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, GSA Advantage pricing, NG911 publicly available cost studies
- Hardware Assumption(s):
  - o Hardware costs include one-time procurement costs, recurring maintenance costs and recurring refresh costs. The application servers are scaled based on the size of the core. Each core will require two servers for redundancy.
- Hardware Methodology:
  - o The equations for hardware costs are shown below.
    - One-time server procurement cost = ((quantity of core * number of servers * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - Refresh cost = (total procurement cost + installation cost)
- Software Assumption(s):
  - o This element requires software costs for data analytics and performance functionality. Software costs include annual licensing fees and are scaled based on the size of the core.
- Software Methodology:
  - o The equation for software costs is shown below.
    - One-time logging and event manager software cost = ((quantity of core * unit cost) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - o This element requires service costs for hardware installation.
- Service Methodology:
  - o The equation for service costs is shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.4.8. FOREST GUIDE

The Forest Guide is a database of geographic data used to route calls to the proper PSAP. The Forest Guide will be implemented at national and state levels with access by regional, state, and local entities.[103] Each successive level will have more precise geographic information.

D.4.8.1.   *Forest Guide in Place*

Geographic data is coalesced at each successive level and a Forest Guide is implemented to allow for more-precise routing between regional and state-level ESInets. The Forest Guide is implemented in the Intermediate stage and continues into the End State stage.

Forest Guide in Place Assumptions

- Primary Source(s):
  - SME input, *2016 National 911 Progress Report*, GSA Advantage pricing
- Hardware Assumption(s):
  - This element requires hardware costs for application servers. These costs include one-time procurement costs, recurring maintenance costs, and refresh costs. The application servers will be at the core level for each region and will be scaled by the size of the core. Each core will require two servers for redundancy.
- Hardware Methodology:
  - The equations for hardware costs are shown below.
    - One-time server procurement cost = ((quantity of cores * number of servers * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - Refresh cost = (total procurement cost + installation cost)
- Service Assumption(s):
  - This element requires service costs for hardware installation.
- Service Methodology:
  - The equation for service costs is shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

---

[103] "Requirements for a National Forest Guide," National Emergency Number Association, August 14, 2014, https://www.nena.org/?NatlForestGuide.

D.4.8.2. National-level Forest Guide in Place

Geographic data is coalesced at each successive level and a national-level Forest Guide is implemented to allow for routing between regional and state-level ESInets. The national-level Forest Guide is implemented in the End State stage.

National-level Forest Guide in Place Assumptions

- Primary Source(s):
    - o SME input, GSA Advantage pricing
- Hardware Assumption(s):
    - o This element requires hardware costs for application servers. These costs include one-time procurement costs, recurring maintenance costs, and refresh costs. The application servers will be at the nationwide level for each region and will be scaled based on the size of the core. This cost includes redundancy.
- Hardware Methodology:
    - o The equations for hardware costs are shown below.
        - One-time server procurement cost = ((quantity of core * number of servers * unit cost) * (1-FC NG911 Current Status%))
        - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
        - Refresh cost = (total procurement cost + installation cost)
- Service Assumption(s):
    - o This element requires service costs for hardware installation.
- Service Methodology:
    - o The equation for service costs is shown below.
        - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.5. INFRASTRUCTURE DOMAIN

The Infrastructure Domain describes the infrastructure elements that interconnect Next Generation Core Services (NGCS) of the Applications and Systems Domain.

Infrastructure Domain Assumptions
The cost assumptions and methodologies used in the model are listed later in this section. The cost assumptions and methodologies are listed at the element level and are segmented by cost type.

Table D-16 shows those cost types included in the Infrastructure Domain at each element level. Costs include hardware, software, services, staff, and facility.

Table D-16: Cost Types for Infrastructure Domain

Cost Element Structure for Infrastructure Domain	Stage	Cost Type				
		Hardware	Software	Services	Staff	Facility
Data Centers						
Gateway Data Centers in Service	Foundational					x
Core Data Centers in Service	Foundational	x		x		x
Ingress Network						
Selective Router to NG911 Network Gateway	Foundational	x		x	x	
Direct Connection to NG911 Network Gateway	Intermediate			x		
Direct Connection using SIP	End State	x		x		
Egress Network						
Legacy PSAP Gateways	Foundational	x		x		
ESInet						
Dedicated Public Safety Network Shared by PSAPs	Foundational	x		x		
National Level ESInet	End State	x		x		x
Network Operations Center (NOC)						
Network Operations Center Monitoring and Maintaining Network	Foundational	x	x	x		
National NOC	End State	x	x	x		
Non-Voice Request for Service						
Shared Standard-based Direct Connection	Intermediate		x			
Network-to-Network Interface						
Limited Interconnections to Other Systems	Foundational			x	x	
Regional Interconnections to Other Systems	Intermediate			x	x	

Table D-17 shows the total Infrastructure Domain costs by cost type for the state implementation and multistate implementation scenarios. Due to the nature of service solution cost calculations, those results are not broken out by the cost type.

Table D-17: NG911 Total Costs for Infrastructure Domain by Cost Type

Cost Type	State Implementation Scenario	Multistate Implementation Scenario
Facilities	$83.3M	$60.2M
Hardware	$303.3M	$206.5M
Services	$2,751.9M	$2,645.3M
Staff	$28.8M	$28.8M
Software	$47.1M	$42.3M
Grand Total	**$3,214.4M**	**$2,983.1M**

Table D-18 indicates the current state of the NG911 functional components for the Infrastructure Domain at the national level. The total progress is shown as 1-FC NG911 Current Status% within the subsequent cost formulas.

Table D-18: Infrastructure Domain NG911 Functional Components Current Status

	Legacy	**Foundational**	**Transitional**	**Intermediate**	**End State**
Data Center	75.4%	24.6%			
Ingress Network	85.7%	9.2%		5.1%	
Egress Network	85.2%	7.2%		7.6%	
ESInet	78.4%	21.6%			
Network Operations Center (NOC)	80.8%	19.2%			
Non-voice Requests for Service	100%				
Network-to-Network Interface (NNI)	100%				
PSAP-to-Responder Network	100%				

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

D.5.1. DATA CENTER

Data centers contain many types of NG911 systems and equipment.

D.5.1.1. Gateway Data Centers

During the course of NG911 implementation, gateways will be hosted in data centers to support the NG911 call flow. These may or may not be colocated with the NGCS. Gateways convert TDM voice calls to SIP for transport across the ESInet. There are three types of gateways: legacy network gateways (LNGs), legacy selective router gateways (LSRGs), and LPGs. Gateways will be implemented in the Foundational stage and continue to operate through the majority of the Transitional stage; gateways should be decommissioned by the end of the Intermediate stage within an area.

Gateway Data Centers Assumptions

This element represents additional space within data centers for necessary equipment to establish network paths for the transition to full ESInet. Hardware necessary to establish these gateways is contained within the Ingress Networks and Egress Networks elements.

- Primary Source(s):
  - o SME input, *2016 National 911 Progress Report*, GSA Advantage pricing
- Hardware Assumption(s):
  - o Related costs are captured in the Selective Router to NG911 Network Gateway element, as well as the Applications and Systems Domain. Therefore, they are not costed out in this element.
- Service Assumption(s):
  - o Service costs (e.g., cooling power and associated maintenance, power, generator) are bundled into the facility costs.
- Facility Assumption(s):
  - o This element requires facility space for the LNGs and LSRGs. The cost is scaled by the number of needed gateways per area.
  - o The required data centers must meet the requirements of either a tier 3 or tier 4 data center standard[104]. The utilized space cost for this study is the average of tier 3 and tier 4 data centers.
  - o The model assumes when space for NG911 data centers is needed that the same floor space, regardless of the data center size, would be sufficient and appropriate. Table D-19 provides the floor space square footage used in the model.

Table D-19: Data Center Costs[105]

	Small Data Center	**Medium Data Center**	**Large Data Center**
Area	12' x 18'	12' x 18'	12' x 18'
Non-recurring Unit Cost	$2,522	$2,522	$2,522
Recurring Unit Cost	$400	$400	$400

---

[104] Tier 3: Meets or exceeds all Tier 2 requirements; Multiple independent distribution paths serving the IT equipment. All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture. Concurrently maintainable site infrastructure with expected availability of 99.982%. Tier 4: Fully redundant in terms of electrical circuits, cooling, and network; architecture can withstand serious technical incidents without server availability ever being affected. The highest level of guarantee: 99.99% availability.

[105] Annual costs for data centers provided by SMEs.

- Facility Methodology:
  o The equations for facility costs are shown below.
    ▪ One-time floor space setup cost = ((quantity of data centers * floor space unit cost) * (1-FC NG911 Current Status%))
    ▪ Annual floor space cost = ((quantity of data centers * recurring floor space unit cost) * (1-FC NG911 Current Status%))

D.5.1.2. Core Data Centers

NGCS data centers host the equipment for security and call-routing functions related to emergency calls, regardless of the incoming call type (e.g., voice, text, multimedia, telematics). NGCS systems are software-driven, requiring highly available servers. These servers must reside in secure, redundant, and resilient data centers. Core data centers will be implemented in the Foundational stage and continue through the End State stage.

Core Data Centers Assumptions
This element represents the equipment and data center space necessary for the initiation of the NGCS, implementing its primary functionality. Additional equipment for other functions is contained within identified specific elements.

- Primary Source(s):
  o SME input, GSA Advantage pricing
- Hardware Assumption(s):
  o This element requires core data center hardware. This cost is scaled based on the number of cores per area. These costs also include one-time procurement costs, recurring maintenance costs, and refresh costs.
- Hardware Methodology:
  o The equations for hardware costs are shown below.
    ▪ One-time hardware procurement cost = ((quantity of core * unit cost) * (1-FC NG911 Current Status%))
    ▪ Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    ▪ Refresh cost = (total procurement cost + installation cost)
- Service Assumption(s):
  o Service costs that pertain to the core data center facility (e.g., cooling power and associated maintenance, power, generator) are bundled into the facilities costs.
  o This element also includes service costs for hardware installation.
- Service Methodology:
  o The equation for service costs is shown below.

- - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))
- Facility Assumption(s):
  - o This element requires facility costs for data centers. The data centers house the redundant NGCS elements to provide the necessary resiliency and backup.
  - o Two data centers are assumed to be the minimum requirement for each state within a region.
  - o The cost is scaled by the number of cores per region and includes one-time setup costs and annual maintenance costs.
  - o The required data centers must meet the requirements of either a tier 3 or tier 4 data center standard. The utilized space cost for this study is the average of tier 3 and tier 4 data centers and is listed in Table D-20.

Table D-20: Data Center Costs[106]

	Small Data Center	**Medium Data Center**	**Large Data Center**
Area	12' x 18'	12' x 18'	12' x 18'
Non-recurring Unit Cost	$2,522	$2,522	$2,522
Recurring Unit Cost	$400	$400	$400

- Facility Methodology:
  - o The equations for hardware costs are shown below.
    - One-time floor space setup cost = ((quantity of data centers * numbers of states per region * floor space unit cost) * (1-FC NG911 Current Status%))
    - Annual floor space cost = ((quantity of data centers * number of states * recurring floor space unit cost) * (1-FC NG911 Current Status%))

D.5.2. INGRESS NETWORK

Ingress networks deliver the incoming calls (e.g., voice, text, multimedia, telematics) to the ESInet.

D.5.2.1.   TDM Connectivity

Time Division Multiplexing (TDM) connectivity delivers calls to the legacy selective routers located at CSP central offices. Centralized automatic message accounting (CAMA) trunks deliver TDM voice calls and their associated automatic number identification (ANI) data from the selective routers to the PSAPs. TDM connectivity is a Legacy stage technology.

---

[106] Annual costs for data centers provided by SMEs.

This represents a legacy capability and, therefore, has no additional costs for NG911.

D.5.2.2. *Selective Router to NG911 Gateway*

Voice calls are delivered from the legacy selective routers (LSRs) in the originating service environment (OSE) to LNGs and LSRGs via multi-frequency (MF) or Signaling System 7 (SS7) trunks for conversion to VoIP signaling and media. Call delivery from selective routers to NG911 gateways is performed in the Foundational stage through the Transitional stage.[107]

Selective Router to NG911 Gateway Assumptions
This initiates a new suite of equipment for a gateway, whose facility cost is contained in the Gateway Data Centers, and the switching of SS7 trunks that no longer will need to connect to the PSAPs.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, *2016 National 911 Progress Report*, vendor pricing, GSA Advantage pricing
- Staff Assumption(s):
  - This element will have FTE staffing costs at the regional level for overseeing administrative work for service level agreements (SLAs) and legal agreements between providers.
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE Staff – 0.1 FTE
  - Percent of year – 100 percent
- Staff Methodology:
  - The equation for staffing costs is shown below.
    - Regional level staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of regions) * (1-FC NG911 Current Status%))

---

[107] "NG9-1-1 Transition Planning Considerations," National Emergency Number Association, November 20, 2013, http://www.nena.org/?page=NG911_TransitionPlng.

- Hardware Assumption(s):
  o This element requires hardware costs for LNGs and gateway data center hardware.
  o These costs also include one-time procurement costs and recurring maintenance costs. Hardware refresh costs are not included in this element because the hardware only is required as an interim phase and will be phased out when the region reaches the End State stage.
- Hardware Methodology:
  o The equations for hardware costs are shown below.
    ▪ One-time server procurement cost = ((quantity of gateways * complexity of gateways * unit cost) * (1-FC NG911 Current Status%))
    ▪ Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  o This element requires service costs for SS7 trunks to add circuits from selective routers to LNGs and LSRGs.
  o This cost includes a one-time trunk installation, which is based on the number of selective routers at the regional level. It also includes a recurring fee that has an initial cost, plus an additional fee that is scaled based on the number of trunk miles per region.
  o This element also includes service costs for hardware installation.
- Service Methodology:
  o The equations for service costs are shown below.
    ▪ One-time trunk cost = ((quantity of selective routers * unit cost) * (1-FC NG911 Current Status%))
    ▪ Annual trunk costs = ((quantity of selective routers * unit cost) * (1-FC NG911 Current Status%))
    ▪ Additional mileage trunk cost = ((average trunk mile * total trunk miles * unit cost) * (1-FC NG911 Current Status%))
    ▪ Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.5.2.3.   *Direct Connection to NG911 Gateway*

Voice calls are delivered from the OSE to LNGs and LSRGs via MF or SS7 trunks for conversion to VoIP signaling and media. Text and other non-voice call types are delivered via IP connections from the CSPs to the Border Control Function (BCF) at the edge of the ESInet. Direct connection from the OSE to the NG911 gateways is performed in the Intermediate stage. This establishes the ability for the selective routers and CAMA trunks to be phased out in favor of direct connections from CSP central offices to the LNGs, and removed entirely with direct SIP connections.

Direct Connection to NG911 Gateway Assumptions

This element includes the engineering and implementation of some new connections by the OSEs to bypass and eliminate the selective routers and fees.

- Primary Source(s):
  - SME input, U.S. Census, *2016 National 911 Progress Report*, *Voice Telephone Services* report (2015), *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, vendor pricing
- Service Assumption(s):
  - This element includes service costs for an OSE's engineers to change connections from selective routers to the legacy gateways. This includes development, engineering, and system testing of the new connection to the gateway.
  - This element also requires service costs for duplicating and moving trunks from the selective routers to the gateway. Overall time for these duplicate trunks for testing periods is assumed to be the same as with the engineering service efforts, and then the ongoing costs are expected to be similar to the existing trunk costs which will be disconnected.
- Service Methodology:
  - The equations for service costs are shown below.
    - Network gateway connections = ((quantity of CSP * unit cost) * (1-FC NG911 Current Status%))
    - Selective router connections operational costs = ((quantity of selective routers * unit costs) * (1-FC NG911 Current Status%))

D.5.2.4. Direct SIP Connections

All emergency calls, regardless of type, are delivered from the OSE to the BCF at the edge of the ESInet.

Direct SIP Connections Assumptions

- Primary Source(s):
  - SME input, *2016 National 911 Progress Report*, *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, vendor pricing, GSA Advantage pricing
- Hardware Assumption(s):
  - This element requires no cost. The LPG equipment for TDM conversion will be phased out based on the ten-year timeline, eliminating those costs for regions that started early deployment.

o   Regions that start implementation five to six years after the start year will be able to skip the Selective Router to NG911 Network Gateway and Direct Connection to NG911 Network Gateway elements.

D.5.3. EGRESS NETWORK

The egress networks connect traffic from the NGCS to legacy PSAPs and to non-911 systems and PSAP networks, which enables legacy PSAPs to receive calls from the NGCS and other PSAPs, and to conference in or transfer calls to third parties outside the NG911 system. Two examples of third parties are language lines and poison-control centers. The legacy network uses administrative lines to connect to agencies via ten-digit dialing. Connections to other PSAPs on the same selective router are handled with star (*) or pound (#) codes across the CAMA trunks.

D.5.3.1.   TDM Connectivity

TDM connectivity to the legacy tandems located at CSP central offices exists to provide legacy telephone connectivity for outbound calls and to allow conferencing with outside agencies, such as a language service or poison control. CAMA trunks enable the transfer of 911 voice calls and their associated ANI data back through the selective routers to other PSAPs. TDM connectivity is a Legacy stage technology.

TDM Connectivity Assumptions
This represents a legacy capability and, therefore, has no additional costs for NG911.

D.5.3.2.   Legacy PSAP Gateway

Legacy PSAPs connected to the NGCS will use LPGs to convert VoIP calls to TDM. Similarly, outbound VoIP-to-TDM trunks are provisioned on the LNGs and LSRGs to handle calls from the ESInet back into the legacy TDM network. Legacy gateways are provisioned in the Foundational stage through the Transitional stage. The LPGs will be removed by the Intermediate stage.

Legacy PSAP Gateway Assumptions
An LPG will be assumed to consist of equipment that typically will be colocated at the PSAPs for the conversion of data from TDM to VoIP. In addition, with this element, PSAPs first will implement IP connectivity to the NGCS; therefore, this element includes digital bandwidth for each PSAP.

- Primary Source(s):
  - o   SME input, *2016 National 911 Progress Report*, *Voice Telephone Services* report (2015), GSA Advantage pricing

- Hardware Assumption(s):
  - o This element includes TDM conversion hardware with the device size and cost based on the number of ports needed at the PSAP level, which is scaled based on PSAP size for each area and listed in Table D-21.

Table D-21: TDM Converter Unit Cost

PSAP Size	TDM Converter Size	Device Quantity	Unit Cost
Small	Small	1.5	$1,435
Medium	Small	1.5	$1,435
Large	Large	1.5	$2,573
Mega	Mega	1.5	$4,941

  - o Hardware costs include one-time procurement costs and recurring maintenance costs. Hardware refresh costs are not included in this element because the hardware only is required as an interim phase and will be phased out when the area reaches the End State stage.
  - o This element also requires a small router per PSAP; however, this is covered in the IP Selective Routing element and is not costed out here.
  - o This element requires a network console manager per PSAP to conduct security and management functions, as well as to provide access to equipment when an issue arises. This is included in the managed router costs or within the NOC; therefore, it is not costed out here.
- Hardware Methodology:
  - o The equations for hardware costs are shown below.
    - ▪ One-time hardware procurement cost = ((quantity of PSAP * type of devices * unit cost) * (1-FC NG911 Current Status%))
    - ▪ Annual O&M cost = ((total hardware procurement cost * O&M%) * (1-FC NG911 Current Status%))
- Software Assumption(s):
  - o This element requires software for the gateway conversions of SIP traffic to TDM. However, this already is embedded within the hardware.
- Service Assumption(s):
  - o This element requires service costs for hardware installation.
  - o This element also requires service costs for a new IP connection from the PSAP to the core. This service cost is based on the bandwidth needed for the connections and is scaled based on the four PSAP sizes. Table D-22 shows the bandwidth needed for each PSAP size and assumes that the bandwidth to/from the PSAPs will increase over the

next years. The figures in Table D-22 depict the initial bandwidth for years 1 through 6, modest bandwidth growth for years 7 through 9, and maximum bandwidth for year 10.

Table D-22: IP Connectivity Costs

PSAP Size	Bandwidth (initial)	Bandwidth (modest)	Bandwidth (maximum)	Unit Cost (initial)	Unit Cost (modest)	Unit Cost (maximum)
Small	T1	3 Mbps	10 Mbps	$3,528	$8,760	$20,652
Medium	10 Mbps	20 Mbps	30 Mbps	$20,652	$21,600	$23,580
Large	20 Mbps	40 Mbps	60 Mbps	$21,600	$27,204	$48,804
Mega	40 Mbps	75 Mbps	100 Mbps	$27,204	$50,784	$54,408

- o   As the nation reaches the End State stage, trunks that connect PSAP circuits to selective routers will be removed, thus creating savings not currently captured in the results.
- Service Methodology:
  - o   The equations for service costs are shown below.
    - ▪   Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))
    - ▪   Annual IP connectivity cost = ((quantity of PSAP * number of links * unit cost) * (1-FC NG911 Current Status%))

D.5.3.3.   PSAP Direct/Outbound Gateways

PSAP equipment is directly connected and processing all traffic in IP and SIP. Outbound VoIP-to-TDM trunks remain provisioned on the LNGs and LSRGs to handle calls from the ESInet back into the legacy TDM network. PSAPs are connected via SIP, but outbound gateways remain in the Intermediate stage.

PSAP Direct/Outbound Gateways Assumptions
Cost savings are captured in the Direct Connection using SIP element as PSAP gateways are phased out.

D.5.3.4.   Direct Connection via SIP

All outbound calls will be handled on VoIP trunks through the BCF. Gateways no longer will be required in the End State stage.

Direct Connection via SIP Assumptions
This element represents no additional costs for the network, only the elimination of previously needed equipment at the PSAPs.

- Hardware Assumption(s):
  - o   This element removes TDM conversion gateway equipment for each PSAP.
- Hardware Methodology:
  - o   Hardware O&M costs are removed with the end of the Intermediate stage for an area.

D.5.4. ESINET

The Emergency Services IP network (ESInet) is the underlying IP network, built to public safety-grade standards, and which supports the systems and services required to deliver calls to the PSAPs.

D.5.4.1.   *Dedicated Network for PSAPs*

Local, regional, and state ESInets are designed, built, and tested. NGCS are installed, configured, and tested across the ESInets. Live 911 calls now traverse the ESInet for delivery to PSAPs. Independent ESInets are deployed in the Foundational stage and remain through the Intermediate stage.

Dedicated Network for PSAPs Assumptions
This element captures the remaining IP networking and equipment components not specifically captured within other areas of the estimate.

- Primary Source(s):
  - o   SME input, *2016 National 911 Progress Report*, *Voice Telephone Services* report (2015), vendor pricing, GSA Advantage pricing
- Hardware Assumption(s):
  - o   This element requires hardware costs for PSAP edge networking equipment. This element is scaled based on the number of PSAPs per region. These costs also include one-time procurement costs, recurring maintenance costs, and refresh costs.
  - o   This element uses routers included in the IP Selective Routing element within the Applications and Systems Domain; therefore, router costs will not be included here.
  - o   This element uses networking security and firewall components included within the Security Domain; therefore, these costs will not be included here.
- Hardware Methodology:
  - o   The equations for hardware costs are shown below.

- One-time hardware procurement cost = ((quantity of PSAPs * number of devices * unit cost) * (1-FC NG911 Current Status%))
- Annual O&M cost = ((total hardware procurement cost * O&M%) * (1-FC NG911 Current Status%))
- Refresh cost = (total procurement cost + installation cost)
- Service Assumption(s):
  - This element requires service costs for bandwidth for core-to-core connectivity, gateway-to-core connectivity, and PSAP connectivity. These costs are scaled based on the number of links per area. If an area only has one core, then the model assumes that a redundant link is accounted for within the Legacy PSAP Gateway element.
  - This element requires service costs for hardware installation.
- Service Methodology:
  - The equations for service costs are shown below.
    - Annual bandwidth cost = ((number of links * number of units * unit cost) * (1-FC NG911 Current Status%))
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.5.4.2. Interconnected Networks

Local, regional, and state ESInets are interconnected and permit other public safety traffic in addition to 911 calls, such as shared incident data and radio traffic. Interconnected ESInets will begin to appear early in the Intermediate stage, but are complete in the End State stage.

Interconnected Networks Assumptions
Transport costs already are captured in the Egress functional component; therefore, it is not costed out here.

D.5.4.3. Nationwide ESInet

The regional and state ESInets need access to a higher-level network to reach agencies outside their area. The nationwide ESInet will be the network of networks that integrates and interconnects the state and regional ESInets, and will exist in the End State stage.

Nationwide ESInet Assumptions
This element includes equipment for the equivalent of two NGCS nodes at the nationwide level and the networking connectivity to all states.

- Primary Source(s):
  - SME input, _2016 National 911 Progress Report_, GSA Advantage pricing

- Hardware Assumption(s):
  o This element requires hardware costs for core data centers at the national level. There will be two national level cores to cover the entire U.S. call handling, thus eliminating other region-to-region transports.
  o These costs include one-time procurement costs, recurring maintenance costs, and refresh costs.
- Hardware Methodology:
  o The equations for hardware costs are shown below.
    ▪ One-time equipment procurement cost = ((quantity of cores * unit cost) * (1-FC NG911 Current Status%))
    ▪ Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    ▪ Refresh cost = (total procurement cost + installation cost)
- Service Assumption(s):
  o This element requires service costs for hardware installation.
  o This element requires service costs for connecting the cores at each region. There will be two connections for each region, which includes redundancy. Additionally, implementation of this element could eliminate other region-to-region transports, but was not captured in the model and could affect the Network-to-Network Interface (NNI) element.
- Service Methodology:
  o The equation for service costs is shown below.
    ▪ Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))
    ▪ Annual bandwidth cost = ((quantity of links * number of regions * unit cost) * (1-FC NG911 Current Status%))
- Facility Assumption(s):
  o This element requires facility costs for two core data centers at the national level.
  o The cost is scaled by two based on the number of national NGCS nodes. Core data centers require tier 3 or tier 4 data center standards. For this cost study, the costs for tier 3 and tier 4 data centers are averaged.
- Facility Methodology:
  o The equations for facility costs are shown below
    ▪ One-time floor space setup cost = ((quantity of cores * floor space unit cost) * (1-FC NG911 Current Status%))
    ▪ Annual floor space cost = ((quantity of cores * recurring floor space unit cost) * (1-FC NG911 Current Status%))

D.5.5. NETWORK OPERATIONS CENTER

The NOC monitors the networks and systems 24 hours a day, 7 days a week (24 x 7), originates and manages trouble tickets with the appropriate service provider or vendor, reports on the health of the networks and systems, and reports on trouble ticket resolution and status.

D.5.5.1. *NOC Network Monitoring*

The NOC monitors networks for trouble and dispatches appropriate resources to resolve the problem. The NOC typically provides regular management reports regarding its activities. The NOC will be required to monitor and manage the ESInet from its initial installation through its lifetime. SLAs will govern problem severity, response times, and reporting. One or multiple NOCs will be deployed in the Foundational stage and continue through the End State stage.

NOC Network Monitoring Assumptions

- Primary Source(s):
  - o SME input, *2016 National 911 Progress Report*, GSA Advantage pricing
- Staff Assumption(s):
  - o This element uses maintenance staff from the Monitoring, Incident, Management and Response element; therefore, it will not be costed out in this element.
- Hardware Assumption(s):
  - o This element requires hardware costs for workstations, which include servers, computers, monitors, and liquid crystal displays (LCD). The hardware costs are based on the number of cores in an area and are scaled based on core size. These costs include one-time procurement costs, recurring maintenance costs, and refresh costs. Table D-23 shows the scale and quantity, by core size, for the hardware that comprises the workstation.

Table D-23: NOC Hardware Scale

	Small NOC	**Medium NOC**	**Large NOC**
Server Type	Medium	Medium	Large
Servers	2	3	2
Personal Computers (PCs)	2	3	4
LCDs	4	4	8
Video Controllers	4-Channel	4-Channel	8-Channel

- Hardware Methodology:
  - o The equations for hardware costs are shown below.
    - One-time procurement cost = ((quantity of core * number of hardware * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - Refresh cost = (total procurement cost + installation cost)
- Software Assumption(s):
  - o This element requires software costs for logging and event manager software. It is based at the core level and is scaled based on the number of nodes or endpoints needed to support devices.
- Software Methodology:
  - o The equations for software costs are shown below.
    - One-time logging and event manager software cost = ((number of nodes * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%)*(1-FC NG911 Current Status%))
- Service Assumption(s):
  - o This element requires service costs for hardware installation.
  - o The element requires service costs for network software setup.
- Service Methodology:
  - o The equations for service costs are shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))
    - Network software setup cost = ((quantity of core * unit cost) * (1-FC NG911 Current Status%))
- Facility Assumption(s):
  - o This element uses facilities from the Monitoring, Incident, Management and Response element; therefore, it will not be costed out in this element.

D.5.5.2. *National-level NOC*

The national-level NOC will have an overarching view of the networks at all levels and will be able to advise subordinate NOCs of issues in their areas. The NOC typically provides regular management reports regarding its activities. SLAs will govern problem severity, response times, and reporting. The national-level NOC will be deployed in the End State stage.

National-level NOC Assumptions

- Primary Source(s):
  o SME input, GSA Advantage pricing
- Hardware Assumption(s):
  o This element requires hardware costs for workstations, which include servers, computers, monitors, and LCDs. The hardware costs are scaled from the large core. These costs include one-time procurement costs, recurring maintenance costs, and refresh costs. Table D-24 shows the scale and quantity, by core size, for the hardware that comprises the workstation.

Table D-24: NOC Hardware Scale

	Small NOC	Medium NOC	Large NOC
Server Type	Medium	Medium	Large
Servers	2	3	2
PCs	2	3	4
LCDs	4	4	8
Video Controllers	4-Channel	4-Channel	8-Channel

- Hardware Methodology:
  o The equations for hardware costs are shown below.
    ▪ One-time procurement cost = ((quantity of core * number of hardware * unit cost) * (1-FC NG911 Current Status%))
    ▪ Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    ▪ Refresh cost = (total procurement cost + installation cost)
- Software Assumption(s):
  o This element requires software costs for logging and event manager software. It is based at the core level and is scaled based on the number of nodes or endpoints needed to support devices.
- Software Methodology:
  o The equations for software costs are shown below.
    ▪ One-time logging and event manager software cost = ((number of nodes * unit cost) * (1-FC NG911 Current Status%))
    ▪ Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))

- Service Assumption(s):
  - o This element requires service costs for hardware installation.
  - o The element requires service costs for network software setup.
- Service Methodology:
  - o The equations for service costs are shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))
    - Network software setup cost = ((quantity of core * unit cost) * (1-FC NG911 Current Status%))

D.5.6. NON-VOICE REQUESTS FOR SERVICE

Non-voice requests for service are machine-to-machine calls, such as those generated by alarm or telematics systems. These calls may be routed differently than a voice call.

D.5.6.1.   Silo and Proprietary Systems

These call types typically are handled by a third-party system, such as a central station monitoring system or a call center, which then contacts the appropriate PSAP and relays the pertinent information. Silo and proprietary systems are in place in the Legacy stage and continue into the Intermediate stage.

Silo and Proprietary Systems Assumptions
This element is at the Legacy state and, therefore, was not costed out.

D.5.6.2.   Shared Standards-based Connections

Proprietary systems are replaced by standards-based systems, and all non-voice requests for service are delivered via standards-based NG911 systems to the appropriate PSAP. Shared standards-based systems will begin deployment in the Intermediate stage and will continue through the End State stage.

Shared Standards-based Connections Assumptions

- Primary Source(s):
  - o SME input, GSA Advantage pricing
- Software Assumption(s):
  - o This element requires software costs to upgrade CPE software at PSAP workstations, which is found in the IP-Based Call-Handling Systems element.

- Software Methodology:
  - o The equation for software costs is shown below.
    - One-time CPE software upgrade = ((total procurement cost * upgrade%) * (1-FC NG911 Current Status%))

D.5.7. NETWORK-TO-NETWORK INTERFACE

The NNI connects disparate service providers' networks to each other, with appropriate safeguards at the interconnection point and within the respective systems to protect both networks. The NNI will be used between ESInets of different providers and states, but also between emergency service networks, additional data systems, and responder networks, to include the First Responder Network Authority (FirstNet) Nationwide Public Safety Broadband Network (NPSBN).

D.5.7.1.   Limited Interconnection

Service providers will implement IP connections between their respective data networks to allow traffic to flow from one network to another network. Interconnections may use proprietary interfaces and be limited in volume. Limited interconnection will be in place from the Foundational stage through the Transitional stage.

Limited Interconnection Assumptions
This element includes staff to initiate information connectivity to a neighboring state and the monthly service cost of maintaining that connectivity. As each state has a connection, when each state implements and maintains the connection, there is redundancy.

- Primary Source(s):
  - o SME input, *2016 National 911 Progress Report*, GSA Advantage pricing
- Staff Assumption(s):
  - o This element requires staff costs for project management, testing, and software and networking engineering. These costs include one-time costs as well as recurring costs. The cost is based on the number of limited interconnections and is scaled at the core level. The assumption is that there will be two connections implemented for each state within an area.
- Staff Methodology:
  - o The equation for staff costs is shown below.
    - One-time staff costs = ((number of states * number of connections * unit cost) * (1-FC NG911 Current Status%))
- Service Methodology:
  - o Annual Service costs = ((quantity of cores * number of connections * unit cost) * (1-FC NG911 Current Status%))

- Other Cost Assumption(s):
  - o This element uses hardware and software from the Security Domain. Therefore, no additional costs of these types are included within this element.

D.5.7.2.   *Regional Interconnections*

Interconnections between systems begin to expand and make use of standards-based NNI connections between service providers, NG911 systems, and their respective data networks, and allow standards-based traffic to flow from one network to another network. Regional interconnections will be in place during the Intermediate stage.

Regional Interconnections Assumptions
This element extends the connectivity to four neighboring states with the same methodology. It requires one-time and annual government FTE staff effort for project management, testing, and software and networking engineering.

- Primary Source(s):
  - o SME input, GSA Advantage pricing
- Staff Assumption(s):
  - o The costs are based on the number of limited interconnections of neighboring regions and are scaled at the core level. The model assumes that the average state would be connected to four neighboring states.
- Staff Methodology:
  - o The equations for staff costs are shown below.
    - ▪ One-time staff costs = ((quantity of cores * number of neighboring connections * unit cost) * (1-FC NG911 Current Status%))
    - ▪ Annual staff costs = ((quantity of cores * number of neighboring connections * unit cost) * (1-FC NG911 Current Status%))
- Hardware Assumption(s):
  - o This element uses hardware from the Security Domain. Therefore, it will not be costed out in this element.
- Software Assumption(s):
  - o This element uses software from the Security Domain. Therefore, it will not be costed out in this element.

D.5.7.3.   *Seamless Interconnection*

Seamless, standards-based NNI connections between the service providers, NG911 systems, responder networks, and their respective data networks allow standards-based traffic to flow from one network to another network. Seamless interconnection will exist in the End State stage.

Seamless Interconnection Assumptions
All systems operate under common standards-based protocols. This element was not costed out for this analysis due to the ongoing development of these standards.

D.5.8. PSAP-TO-RESPONDER NETWORK

The PSAP-to-responder network transfers information from the PSAP to responders in the field.

D.5.8.1.   Silo and Proprietary Systems

Responder communications use locally or regionally controlled independent systems, such as land mobile radio (LMR) or mobile data terminals connected to a local CAD system. Silo systems are in place in the Legacy stage and will continue into the Intermediate stage.

Silo and Proprietary Systems Assumptions
This element is at the Legacy stage and, therefore, was not costed out.

D.5.8.2.   Shared Standards-based System

PSAPs are connected to responders with standards-based systems that will allow information flow, such as the systems envisioned by FirstNet. Shared NG911 systems will be implemented beginning in the Intermediate stage and will be completed in the End State stage.

Shared Standards-based System Assumptions
Standards are not in place for this element; therefore, this element was not costed out. This will include, in the future, FirstNet and other responder communications networks and applications.

D.6.   SECURITY DOMAIN

The Security Domain encompasses the network, facility, and personnel security associated with the implementation of NG911 services. Specifically, this domain focuses on the policies, systems, and applications required to develop the access, network, and information security appropriate for each stage of the NG911 Security Model. Security is designed into the NG911 systems and most of the standards reflect this security by design. National Emergency Number Association (NENA) standards require the use of Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) protocols between systems within an ESInet, and require authentication and authorization for access to systems and data.

The NENA i3 standard implements most of its network and information security controls by passing all NG911 traffic through the BCF. Access to the NG911 systems and applications is mainly controlled by operating system-level credentialing that replicates hierarchically across interconnecting domains, and which enables authorized users to operate at any location.

Security Domain Assumptions

The cost assumptions and methodologies used in the model are listed later in this section. The cost assumptions and methodologies are listed at the element level and are segmented by cost type. Table D-25 shows those cost types included in the Security Domain at each element level. Costs include hardware, software, services, staff, and facility.

Table D-25: Cost Types for Security Domain

Cost Element Structure for Security Domain	Stage	Cost Type				
		Hardware	Software	Services	Staff	Facility
Border Control Function (BCF)						
Border Control Function is Available and Functioning	Transitional	x	x	x		
Facility and Personnel Security						
Local, Regional, or Statewide Single Log-in	Foundational	x		x	x	
Trustmark Access Across All systems	End State	x		x		
Network and Security Monitoring						
Monitoring, Incident, Management and Response	Foundational				x	x
EC3	Intermediate	x	x	x		

Table D-26 shows the total Security Domain costs by cost type for the state implementation and multistate implementation scenarios. Due to the nature of service solution cost calculations, these results are not broken out by the cost type.

Table D-26: NG911 Total Costs for Security Domain by Cost Type

Cost Type	State Implementation Scenario	Multistate Implementation Scenario
Facilities	$10.3M	$2.2M
Hardware	$211.6M	$189.1M
Services	$113.5M	$108.2M
Staff	$403.4M	$97.3M
Software	$493.1M	$220.2M
Grand Total	**$1,231.9M**	**$617.0M**

Table D-27 indicates the current status of the NG911 functional components for the Security Domain at the national level. The total progress is shown as 1-FC NG911 Current Status% within the subsequent cost formulas.

Table D-27: Security Domain NG911 Functional Components Current Status

	Legacy	**Foundational**	**Transitional**	**Intermediate**	**End State**
Border Control Function (BCF)	82.1%		17.9%		
Facility and Personnel Security	97.8%	2.2%			
Network and Security Monitoring	80.8%	19.2%			

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

D.6.1. BORDER CONTROL FUNCTION

The BCF provides perimeter security through its firewall, and VoIP call processing through its Session Border Controller (SBC). All PSAPs that have an externally accessible IP network today already have one or more firewalls, at all levels of the maturity model. But because it is highly desirable that the NG911 connection has its own dedicated firewall to assure homogenous implementation of routing and security rules on the ESInet, the cost model must include additional units for all PSAP and core interconnection points starting at the Transitional stage.

The SBC is necessary to process IP 911 calls and to anchor (temporarily store) the solicited and unsolicited 911 call multimedia content until it is delivered to the appropriate answering position or to another ESInet. The SBC also provides IP packet address conversion, data encryption/decryption, call bridging, quality-of-service processing, call-detail recording, and performance measurements. Intrusion detection and intrusion prevention systems (IDS/IPS) provide additional security in identifying and isolating penetrations of the network perimeter.

D.6.1.1. BCF Available and Functioning

The BCF is installed, configured, and tested. The BCF manages all voice and data traffic entering and exiting the network. The BCF is in place beginning in the Transitional stage and continues throughout the End State stage.

BCF Available and Functioning Assumptions
This element requires firewalls and SBCs for each PSAP and core. This element requires software for firewalls and a separate IPS for each core.

- Primary Source(s):
  - o SME input, *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, GSA Advantage pricing
- Hardware Assumption(s):
  - o Firewalls and SBCs for PSAPs have one-time procurement costs, recurring maintenance costs, and refresh costs. The costs are scaled based on the number and size of PSAPs per area. From a planning perspective, while small PSAPs will have single-path BCFs in place, all others will plan fully redundant paths.
  - o Firewalls and SBCs for cores require hardware redundancy and include one-time procurement costs, recurring maintenance costs, and refresh costs. The costs are scaled based on the number and size of cores per area.
  - o Additionally, a hardware installation factor is included. Along with the hardware cost factor included from the legacy gateway installation, the complete cost of the initial installation at the PSAPs should be represented. Table D-28 shows the hardware costs and hardware quantity for the PSAPs, based on size, and the core.

Table D-28: BCF Hardware Costs

Hardware	Small	Medium	Large	Mega	Core
Firewalls	$2,300	$6,300	$10,200	$10,200	$10,200
SBCs	$2,700	$2,700	$11,800	$11,800	$30,250
Hardware Quantity	1	2	2	2	2
Total Hardware Cost	**$5,000**	**$18,000**	**$44,000**	**$44,000**	**$80,900**

- Hardware Methodology:
  - o The equations for hardware costs are shown below.
    - ▪ One-time BCF PSAP cost = ((quantity of PSAP * number of hardware * unit cost) * (1-FC NG911 Current Status%))
    - ▪ Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))

- Refresh cost = (total procurement cost + installation cost)
- Software Assumption(s):
  - This element requires software costs for firewalls as well as separate IPSs at the PSAP level. These costs are scaled based on the number and size of PSAPs per area. Costs include one-time procurement costs and recurring maintenance costs.
  - This element requires software costs for firewalls as well as IPSs at the core level. All cores require software redundancy. These costs are scaled based on the number and size of cores per area. Costs include one-time procurement costs and recurring maintenance costs. Table D-29 shows software costs for the PSAPs, based on size, and the core.

Table D-29: BCF Software Costs

Software	Small	Medium	Large	Mega	Core
SBC Software	$1,500	$4,880	$38,400	$38,400	$780,000
Software Quantity	1	2	2	2	2
Total Software Cost	**$1,500**	**$9,760**	**$76,800**	**$76,800**	**$1,560,000**

- Software Methodology:
  - The equations for software costs are shown below.
    - One-time software procurement PSAP cost = ((quantity of PSAPs * number of software * unit cost) * (1-FC NG911 Current Status%))
    - One-time software procurement core cost = ((quantity of cores * number of software * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - This element requires service costs for hardware installation.
- Service Methodology:
  - The equation for service costs is shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.6.2. FACILITY AND PERSONNEL SECURITY

From an NG911 perspective, there is physical security, necessary to protect the NG911 system physical infrastructure, and cybersecurity, which requires policies, systems, and software to protect the integrity of the network and the confidential information it carries. Although it is possible to

improve a PSAP's physical security to protect against acts of terror, such security generally is well implemented in legacy PSAPs.

Even in the most optimistic view, physical security will not prevent local, regional, or state NG911 computing or networking components from being compromised, intentionally or accidentally. The NG911 network only can be secured by implementing strong external and internal access controls supported by contemporary security policies that consider the new realities of cybersecurity.

One of the most important requirements for NG911 is that each system user be uniquely identifiable, and that their associated credentials must define their access rights for applications available from the network at that location. Furthermore, access to critical systems such as NG911 must use dual-factor authentication, which provides greater assurance that users are who they say they are, most especially when the system is accessed outside secured facilities, as in the case of mobile devices.

D.6.2.1. *Individual System Log-in*

The individual user has a unique or shared username and password for accessing each 911 application, system, or auxiliary platform. Individual log-in is in place in the Legacy stage.

Individual System Log-In Assumptions
This element is at the Legacy stage and, therefore, was not costed out.

D.6.2.2. *Local, Regional, Statewide Single Log-in*

Each individual user has a unique username and password. This combination provides a single-factor log-in to all authorized 911 applications, systems, and auxiliary platforms, while mobile users would be required to use dual-factor authentication. Single-factor log-in begins in the Foundational stage and continues into the Intermediate stage.

Local, Regional, Statewide Single Log-in Assumptions

- Primary Source(s):
  - SME input, OPM Labor Rates, GS locality factors, GSA CALC, *2016 National 911 Progress Report*, *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, GSA Advantage pricing
- Staff Assumption(s):
  - This element will have FTE security staffing costs for large and mega PSAPs, as well as staff at the core level.

- o The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - o Number FTE Staff – 0.1 FTE
- Staff Methodology:
  - o The equation for staffing costs is shown below.
    - Staffing cost = (((annual labor rate of government employee * locality factor) * number of PSAPs * FTE * duration in % of year) * (1-FC NG911 Current Status%))
- Hardware Assumption(s):
  - o This element requires hardware costs at the PSAP and core level. Hardware costs include servers, workstation equipment e.g., (computers, monitors) and computer fingerprint readers for all workstations. These costs include one-time procurement costs, recurring maintenance costs, and refresh costs.
  - o PSAPs at the hardware level are scaled based on the PSAP size and the number of PSAP positions in the area.
  - o Hardware costs at the core level are scaled based on the number of cores per area. The model assumes that there is redundancy at the core level.
- Hardware Methodology:
  - o The equations for hardware costs are shown below.
    - One-time PSAP hardware procurement cost = (((quantity of PSAPs * quantity of PSAP positions) * number of equipment * unit cost) * (1-FC NG911 Current Status%))
    - One-time core hardware procurement cost = ((quantity of core * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - Refresh cost = (total procurement cost + installation cost)
- Service Assumption(s):
  - o This element requires service costs for hardware installation at the core and PSAP level.
  - o This element requires service costs for contractor network engineers to provide dual identification at the PSAP and at the regional level. PSAP contractor costs are scaled based on the number of PSAPs in an area.
  - o The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these already are defined as national averages.
  - o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.

- o   Number FTE staff – 1 FTE
- o   Percent of year
  - ▪   At PSAP level – 3.8 percent
  - ▪   At regional level – 25 percent
- Service Methodology:
  - o   The equations for service costs are shown below.
    - ▪   Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))
    - ▪   Dual identification contractor cost at core = ((annual contractor rate * FTE * duration in % of year * number of regions) * (1-FC NG911 Current Status%))
    - ▪   Dual identification contractor cost at PSAP = ((annual contractor rate * FTE * duration in % of year * number of PSAPs) * (1-FC NG911 Current Status%))

D.6.2.3.   *Trustmark Access*

Access is advanced to a trustmark framework enabling a scalable, agile environment for managing trusted access to all applicable 911 applications, systems, and auxiliary platforms. User credentials are replicated hierarchically so that NG911 systems and applications can be accessed anywhere authorized. Dual-factor authentication is mandatory across the system. Trustmark access is in place in the End State stage.

Trustmark Access Assumptions

This element puts in place systems at the national cores capable of aggregating and disseminating nationwide trustmark access credentials for emergency communicators.

- Primary Source(s):
  - o   SME input, OPM Labor Rates, GS locality factors, GSA CALC, *2016 National 911 Progress Report*, GSA Advantage pricing
- Staff Assumption(s):
  - o   This element uses staffing contained within the Network and Security Monitoring functional component. Therefore, no additional costs are included within this element.
- Hardware Assumption(s):
  - o   This element requires hardware costs at the national core level. Hardware costs include servers, workstation equipment (e.g., computers, monitors) and computer fingerprint readers for additional security measures. These costs also include one-time procurement costs, recurring maintenance costs, and refresh costs.
  - o   Hardware costs are scaled based on the number of national cores and will include redundancy.
- Hardware Methodology:
  - o   The equations for hardware costs are shown below.

- One-time core hardware procurement cost = ((quantity of core * number of equipment * unit cost) * (1-FC NG911 Current Status%))
- Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
- Refresh cost = (total procurement cost + installation cost)
- Service Assumption(s):
  - This element requires service costs for systems installation at the core level.
  - This element requires service costs for contractor network engineers to provide dual identification at the national core level.
  - The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these already are defined as national averages.
  - The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff – 1 FTE
  - Percent of year – 25 percent
- Service Methodology:
  - The equations for service costs are shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))
    - Dual identification contractor cost at core = ((annual contractor rate * FTE * duration in % of year) * (1-FC NG911 Current Status%))

D.6.3. NETWORK AND SECURITY MONITORING

Network security is not an event, but rather a continuous process. Monitoring for security infractions and network integrity, combined with appropriate incident response, protects NG911 operations. NG911 is currently, and will continue to be, implemented within existing local, regional, and state network infrastructures that have various levels of security rules and enforcement capabilities. Furthermore, many smaller PSAPs have very little exposure to security issues and will need assistance preparing for NG911 system security requirements. To assure the integrity of the national NG911 system, the National 911 Program will need to educate local authorities and PSAP managers about new security policies and audit their readiness.

D.6.3.1. *Monitoring, Incident Management and Response*

Network and security monitoring is operational with a defined incident management process in place. Coordinated response is practiced and executed when network problems and security

infractions arise. Continuous improvement processes are in place to ensure that all incidents are met with comprehensive and effective issue-mitigation techniques.

A hierarchical design for security and network monitoring and management, as well as incident response and resolution, is the preferred methodology for implementation on a national scale. Local and regional network operations centers (NOCs) and/or security operations centers (SOCs) would collect monitoring data at the local and regional level and pass it up to the state level. States would collect the regional data and pass it up to the national level. In some cases, there only may be a state-level NOC/SOC, or an NOC/SOC that monitors and manages a small group of states.

At the national level, there may be two nationwide NOCs/SOCs for redundancy and resiliency, all with overarching access to the same data, and the view of attacks or outages provided by that overarching view.[108]

Network monitoring, incident management, and response are implemented in the Foundational stage and continue throughout the End State stage.

Monitoring, Incident Management and Response Assumptions
This element requires annual government FTE staff effort to coordinate responses during network and security problems. This includes 24-hour staffing at the regional and national level. This element also requires information technology (IT) office space for each core. While workstations and network software services also are required for this element, costs were accounted for in the Network Operations Center functional component.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, GSA CALC, GSA Advantage pricing
- Staff Assumption(s):
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the region. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The model assumes the use of an existing Cyber Emergency Response Team (CERT) in place at the national level; therefore, it was not costed out.
  - This element requires annual service costs for monitoring staff at the regional and national level. The regional level will include staff that operate during business hours, as well as staff that operate 24 x 7.

---

[108] Section 6 of the TFOPA Working Group 1 report presents a conceptual design called Emergency Communications Cybersecurity Center (EC3) structured in this manner.

- o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
- o Two regional 24 x 7 staff – 10 FTEs
  - ▪ Regional business hours staff – The staff number for operating during business hours is based on the number of NOC workstations for an area. This does not include redundancy.
- o National level staff – 5 FTEs
- o Percent of year – 100 percent
- Staff Methodology:
  - o The equation for staffing costs is shown below.
    - ▪ Annual staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year) * (1-FC NG911 Current Status%))
- Hardware Assumption(s):
  - o Related costs are captured in the Network Operations Center functional component within the Infrastructure Domain. Therefore, it is not costed out in this element.
- Service Assumption(s):
  - o Related costs are captured in the Network Operations Center functional component within the Infrastructure Domain. Therefore, it is not costed out in this element.
- Facility Assumption(s):
  - o This element requires IT office space facility costs. These costs are scaled at the core level. The model assumes that each NOC IT office space has a size of 800 square feet and is priced at $32 per square foot.[109]
  - o The model assumes that a CERT already will be in place at the national level. Therefore, it will not be costed out.
- Facility Methodology:
  - o The equation for facility costs is shown below.
    - ▪ Annual office space leasing cost = ((quantity of core * space size * unit cost) * (1-FC NG911 Current Status%))

D.6.3.2. *Emergency Communications Cybersecurity Centers (EC3)*

Network and security monitoring and response are operational with a defined incident management process in place. "The intent of the logical architecture recommendation is to create a centralized function, and location, for securing Next Generation (NG) networks and systems. By centralizing certain features, including cybersecurity in general, and intrusion detection and prevention services (IDPS) specifically, public safety can take advantage of economies of scale,

---

[109] IT office space size and cost per square foot are provided by SMEs.

multiple resources, and systems and best practices which may already be in place or at a minimum readily available for deployment and use."[110]

The EC3 would be able to monitor networks and systems and react quickly to issues. The EC3 would require a method to share and distribute information as needed to ensure that a coordinated response is practiced and executed when network problems and security infractions arise. Continuous improvement processes are in place to ensure that all incidents are met with comprehensive and effective issue-mitigation techniques. In some cases, there only may be a state-level NOC/SOC, or an NOC/SOC that monitors and manages a small group of states.

At the national level, there may be two or more nationwide NOCs/SOCs for redundancy and resiliency, all with overarching access to the same data, and the view of attacks or outages provided by that overarching view.[111]

Full EC3 functions are implemented in the Intermediate stage and continue throughout the End State stage.

EC3 Assumptions
Many functions of the EC3 are included within other elements of the Security Domain. One item not specifically addressed concerns intrusion-detection sensors at each PSAP. This is met by a combination of software at the small PSAPs and physical sensors at all other PSAPs.

- Primary Source(s):
  o SME input, GSA Advantage pricing
- Staff Assumption(s):
  o Related costs are captured in the Monitoring, Incident, Management and Response element. Therefore, it is not costed out in this element.
- Hardware Assumption(s):
  o This element requires hardware costs for IP sensors. These costs are scaled at the core and PSAP level. IP sensors only pertain to mega and large PSAPs. Small and medium PSAPs use intrusion detection and prevention (IDP) software.
  o These costs also include one-time procurement costs, recurring maintenance costs, and refresh costs.
  o Hardware costs are scaled based on the number of cores and PSAPs in an area and will include redundancy.

---

[110] Task Force on Optimal PSAP Architecture, *Cybersecurity: Optimal Approach for PSAPs Supplementary Report*, (December 2, 2016), Working Group 1.
[111] Section 6 of the TFOPA Working Group 1 report presents a conceptual design called Emergency Communications Cybersecurity Center (EC3) structured in this manner.

- Hardware Methodology:
  - o The equations for hardware costs are shown below.
    - One-time core hardware procurement cost = ((quantity of cores * number of sensors * unit cost) * (1-FC NG911 Current Status%))
    - One-time PSAP hardware procurement cost = ((quantity of PSAPs * number of sensors * unit cost) * (1-FC NG911 Current Status%))
    - Annual O&M cost = ((total procurement cost * O&M%) * (1-FC NG911 Current Status%))
    - Refresh cost = (total procurement cost + installation cost)
- Software Assumption(s):
  - o This element requires software costs for IDP software at the PSAP level. These costs only pertain to small and medium PSAPs. They are scaled based on the number of PSAPs per area.
- Software Methodology:
  - o The equation for software costs is shown below.
    - Annual software licensing cost = ((quantity of PSAPs * number of software * unit cost) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - o This element requires service costs for hardware installation at the PSAP and core level.
- Service Methodology:
  - o The equation for service costs is shown below.
    - Installation cost = ((total procurement cost * installation%) * (1-FC NG911 Current Status%))

D.7. OPERATIONS/PERFORMANCE DOMAIN

The Operations/Performance Domain describes the policies, procedures, and programs that are needed to effectively operate NG911 systems.

Operations/Performance Domain Assumptions
The cost assumptions and methodologies used in the model are listed later in this section. The cost assumptions and methodologies are listed at the element level and are segmented by cost type. Table D-30 shows those cost types included in the Operations/Performance Domain at each element level. Costs include services and staff.

Table D-30: Cost Types for Operations/Performance Domain

Cost Element Structure for Operations and Performance Domain	Stage	Cost Type				
		Hardware	Software	Services	Staff	Facility
PSAP Training						
Develop, Implement, and Update PSAP Training	Foundational				x	
Operational Procedures						
Develop, Implement, and Update Operational Procedures	Foundational				x	
Service Level Agreements						
Develop, Implement, and Update Service Level Agreements	Foundational				x	
Contingency Plans						
Develop, Implement, and Update Contingency Plans	Foundational			x	x	
Data QA						
Develop, Implement, and Update Data QA and Analysis	Foundational				x	
System Testing						
Develop, Implement, and Update System Testing	Foundational				x	
Cybersecurity Program						
Coordinated Cross System Cybersecurity Programs	Intermediate				x	

Table D-31 shows the total Operations/Performance Domain costs by cost type for the state implementation and multistate implementation scenarios. Due to the nature of service solution cost calculations, these results are not broken out by the cost type.

Table D-31: NG911 Total Costs for Operations/Performance Domain by Cost Type

Cost Type	State Implementation Scenario	Multistate Implementation Scenario
Services	$224.2M	$216.0M
Staff	$107.8M	$92.9M
Grand Total	**$332.0M**	**$308.9M**

Table D-32 indicates the current status of the NG911 functional component for the Operations/Performance Domain at the national level. The total progress is shown as 1-FC NG911 Current Status% within the subsequent cost formulas.

Table D-32: Operations/Performance Domain NG911 Functional Components Current Status

	Legacy	Foundational	Transitional	Intermediate	End State
PSAP Training	99.6%	0.4%			
Operational Procedures	100%				
Managed Services	100%				
Service Level Agreements (SLAs)	100%				
Contingency Plans	91.7%	8.3%			
Data QA	100%				
System Training	100%				
Cybersecurity Program	92.9%	7.1%			

The NG911 current status defines the current NG911 environment across the nation by displaying the percentage of the population for which NG911 components have been implemented in each domain for each maturity stage.

D.7.1. PSAP TRAINING

Per the National 9-1-1 Assessment Guidelines, "Training should exist and be the same for all staff who perform telecommunicator duties."[112] In the Legacy stage today, the Association of Public-Safety Communications Officials (APCO) and the National Fire Protection Association (NFPA) have training standards for telecommunicators. Some states have rules in place, or are in the process of adopting rules, to mandate state-level training standards. These state and national training standards will need to be updated as NG911 services, such as text, pictures, and video, are introduced.

D.7.1.1. Develop, Implement, and Update PSAP Training

State, tribal, regional, or local 911 authorities will develop or adopt training standards for new types of information being presented to the PSAP. Training will be implemented at the state, regional, or local level in the Foundational stage, and continue to be monitored and updated on an ongoing basis through the End State stage.

---

[112] "Draft Report for National 9-1-1 Assessment Guidelines," 911 Resource Center, June 2012, https://resourcecenter.911.gov/911Guidelines/RPT053012_National_911_Assessment_Guidelines_Report_FINAL.pdf, section 5.6.

Develop, Implement, and Update PSAP Training Assumptions

This element includes staffing for the statewide coordination of ongoing PSAP training handled by the local jurisdictions, which is not part of this cost estimate.

- Primary Source(s):
    - SME input, OPM labor rates, GS locality factors
- Staff Assumption(s):
    - Ongoing training for PSAPs is not costed out, with the exception of one-time development of training for new equipment or systems (e.g., CAD training). Regular staff hours are used for developing and conducting training. Costs are scaled based on the number of cores per area. Redundancy is not costed out in this element.
    - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
    - The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
    - Number FTE staff – 1 FTE
    - Percent of year – 100 percent
- Staff Methodology:
    - The equation for staffing costs is shown below.
        - Staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of cores) * (1-FC NG911 Current Status%))

D.7.2. OPERATIONAL PROCEDURES

Most standard operating procedures (SOPs) are managed at the local PSAP level in the Legacy stage, with some state or regional entities regulating a minimum level of service delivery and/or performance standards.

D.7.2.1. *Develop, Implement, and Update Operational Procedures*

The state or region may develop or update procedures specific to NG911 to include: service delivery, performance, interface standards for data exchange/sharing, call processing, security, redundancy and reliability, and interdependencies between systems. Operational procedures are implemented in the Foundational stage and continue to be monitored and updated on an ongoing basis through the End State stage.

Develop, Implement, and Update Operational Procedures Assumptions
This element requires government FTE staff to develop, implement, and update operational procedures annually at the core level.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors
- Staff Assumption(s):
  - Policy and procedures at the PSAP level are assumed to be a continuation of legacy operations. Costs are scaled based on the number of cores per area. Redundancy is not costed out in this element.
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff – 0.1 FTE
  - Percent of year – 100 percent
- Staff Methodology:
  - The equation for staffing costs is shown below.
    - Staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of cores) * (1-FC NG911 Current Status%))

D.7.3. MANAGED SERVICES

NGCS may be managed and maintained by the 911 authority, or procured in a managed-services contractual arrangement that would include the service offering. Some models also enable a third-party managed-services provider to ensure vendor compliance with SLAs, and to have an additional level of review on the system, allowing for the 911 authority to focus on 911 operations.

D.7.3.1.   *Develop, Implement, and Maintain Managed Services*

Managed services may be deployed in conjunction with an ESInet or NGCS NOC. All NG911 components have a robust managed service provided by the 911 authority, its NGCS/ESInet solution provider, and/or a third party. 911 authorities having complex needs may have managed services provided by two or three potential providers for comprehensive oversight of system performance. Managed services are implemented in the Foundational stage and continue to be monitored and maintained on an ongoing basis through the End State stage.

Develop, Implement, and Maintain Managed Services Assumptions
These costs are accounted for in the ongoing managed services and, therefore, were not costed out in this element.

D.7.4. SERVICE LEVEL AGREEMENTS

NENA recommends that prior to transitioning to NG911, 911 authorities determine the methodology to be used to ensure that network and system operation and reliability meet acceptable and adopted standards.[113] Solutions should provide the capability to monitor, record, and analyze system performance data against predefined metrics (e.g., establish system norms and flag exceptions).

D.7.4.1. *Develop, Implement, and Maintain SLAs*

The state or 911 authority determines and implements, through contract negotiations, the appropriate service levels. SLAs are implemented in the Foundational stage and continue to be monitored and maintained on an ongoing basis through the End State stage.

Develop, Implement, and Maintain SLAs Assumptions
This element requires government FTE staff to develop, implement, and update SLAs annually at the core level.

- Primary Source(s):
  - o SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  - o Costs for this element are ongoing and are scaled based on the number of cores per area. Redundancy is not costed out in this element.
  - o The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - o The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - o Number FTE staff – 0.2 FTE
  - o Percent of year – 100 percent
- Staff Methodology:
  - o The equation for staffing costs is shown below.

---

[113] "NG9-1-1 Planning Guidelines," National Emergency Number Association, January 8, 2014, https://www.nena.org/?page=ng911planning.

- Staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of cores) * (1-FC NG911 Current Status%))

D.7.5. CONTINGENCY PLANS

Contingency planning, often referred to as a continuity of operations plan (COOP), occurs at all levels of the hierarchy, from individual PSAPs to regions to states/territories to the national level. Neighboring PSAPs may come together to review each other's operations, staffing, location, etc. NENA publishes an informational document on contingency and disaster planning to assist 911 entities in developing, implementing, and testing their own plans.

D.7.5.1. Develop, Implement, and Update Contingency Plans

The state or 911 authority develops and implements plans. Contingency plans are living documents and, as such, require regular reviews and updates. Contingency plans are developed in the Foundational stage, and a process of plan, review, update, test, and repeat should occur on an ongoing basis through the End State stage.

Develop, Implement, and Update Contingency Plans Assumptions
This element requires a one-time government FTE staff effort and contractor services to develop a contingency plan, as well as annual government FTE staff and contractor services to implement and update contingency plans, both at the core level.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  - Costs for this element are scaled based on the number of states at the regional level. The costs include one-time staff costs for contingency plan development and annual staff costs for updating the plan. Redundancy is not costed out in this element.
  - The annual staff costs for this element are scaled as a percentage (10 percent annual factor) of the total one-time staff costs.
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE Staff
    - Strong – 0.25 FTE

- ▪ Medium – 0.5 FTE
- ▪ Weak – 0.5 FTE
  - o Percent of year – 100 percent
- Staff Methodology:
  - o The equations for staffing costs are shown below.
    - ▪ One-time staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of cores) * (1-FC NG911 Current Status%))
    - ▪ Annual staffing cost = ((total one-time staffing cost * total one-time staffing cost%) * (1-FC NG911 Current Status%))
- Service Assumption(s):
  - o This element requires one-time service costs for contractors for contingency plan development and annual service costs for updating the plan. The annual cost is a fully burdened rate for a contractor that also includes profit as detailed from the GSA CALC database of labor categories. No locality factor is used with contractor rates as these are already defined as national averages.
  - o The LOE used to calculate the cost is based on the area's category (strong, medium, weak). The category, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - o Number FTE staff
    - ▪ Strong – 2 FTEs
    - ▪ Medium – 3 FTEs
    - ▪ Weak – 6 FTEs
  - o Percent of year – 100 percent
  - o The annual service contractor costs for this element are scaled as a percentage (10 percent annual factor) of the total one-time contractor cost.
- Service Methodology:
  - o The equations for service costs are shown below.
    - ▪ One-time contractor cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of cores) * (1-FC NG911 Current Status%))
    - ▪ Annual contractor cost = ((total one-time staffing cost * total one-time contactor cost %) * (1-FC NG911 Current Status%))

D.7.6. DATA QUALITY ASSURANCE AND ANALYSIS

NENA publishes recommended data requirements and data quality assurance (QA) standards for 911 authorities to adopt. Data quality is monitored and maintained at the local level, and pushed up to successively higher levels in the hierarchy (regional, state, national, and international).

Validation checks are performed at each level to ensure that the data is transferred cleanly and is properly formatted for that level.

D.7.6.1.   Develop, Implement, and Update Data QA

The state or 911 authority will develop or adopt standards for data quality, and develop policies and procedures to manage the data.

Develop, Implement, and Update Data QA Assumptions
This element requires government FTE staff annually to develop, implement, and update data QA and analysis at the core level.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors
- Staff Assumption(s):
  - Costs are ongoing and are scaled based on the number of states at the regional level. Redundancy is not costed out in this element.
  - The default labor used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff – 0.2 FTE
  - Percent of year – 100 percent
- Staff Methodology:
  - The equation for staffing costs is shown below.
    - Staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of cores) * (1-FC NG911 Current Status%))

D.7.7. SYSTEM TESTING

Each system, procedure, and data element is important to NG911 systems. A comprehensive technical system testing program should be in place, including data auditing, system metric testing, and security testing.

D.7.7.1.   Develop, Implement, and Maintain System Testing

The state or 911 authority develops, implements, and maintains comprehensive testing of all systems, data, and procedures to ensure compliance and effectiveness of the NG911 systems. System testing will begin in the Foundational stage and continue through the End State stage.

Develop, Implement, and Maintain System Testing Assumptions
This element will have FTE staff to develop, implement, and update system testing at the regional level.

- Primary Source(s):
  - SME input, OPM labor rates, GS locality factors
- Staff Assumption(s):
  - Costs for this element are ongoing and are scaled based on the number of states at the regional level. Redundancy is not costed out in this element.
  - The default labor rate used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff – 0.5 FTE
  - Percent of year – 100 percent
- Staff Methodology:
  - The equation for staffing costs is shown below.
    - Staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of cores) * (1-FC NG911 Current Status%))

D.7.8. CYBERSECURITY PROGRAM

The development and maintenance of a cybersecurity program is required as 911 authorities begin to operate in an IP-based environment, regardless of whether the operations encompass CAD, radio, or NG911 call delivery and call handling. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[114] provides a structure of functions and categories that may assist 911 authorities in developing a cybersecurity program that captures the methodologies and outcomes that are customized and appropriate for the

---

[114] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, (February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

911 authority's operations. Cybersecurity programs should provide documented breach prevention, mitigation, redundancy, reporting, and recovery procedures.

D.7.8.1.   *Multiple Diverse System Cybersecurity Programs*

IP systems are deployed in silos with limited security services from IP network providers. Cybersecurity processes and awareness are isolated and limited in deployment. Diverse cybersecurity programs will begin to appear in the Foundational stage and continue through the Transitional stage.

Multiple Diverse Cybersecurity Programs Assumptions
This element is at the Legacy stage and, therefore, was not costed out.

D.7.8.2.   *Coordinated Cross-system Cybersecurity Program*

The cybersecurity program across all systems and vendors is ingrained in operations, with maintenance processes established to enable the program to evolve as operations, threats, and vulnerabilities change. Coordinated cross-system cybersecurity programs will begin to appear in the Intermediate stage and continue through the End State stage.

Coordinated Cross-system Cybersecurity Program Assumptions
This element requires government FTE staff annually to coordinate cross-system cybersecurity programs at the regional level.

- Primary Source(s):
  - SME input, OPM Labor Rates, GS locality factors, GSA CALC
- Staff Assumption(s):
  - This element will have FTE staff costs to coordinate cross-system cybersecurity programs.
  - The default labor used for the government FTE is GS-10, which is based off the OPM General Schedule (base) pay table. Each labor rate used in calculating the cost is factored by a locality factor based on the states within a region and includes overhead and fringe benefit costs.
  - Costs are ongoing and are scaled based on the number of cores per region. Redundancy is not costed out in this element.
  - The LOE, labor rate, and percent of year needed to complete the element are identified by SMEs.
  - Number FTE staff – 1 FTE
  - Percent of year – 100 percent

- Staff Methodology:
  - o The equation for staffing costs is shown below.
    - ▪ Staffing cost = (((annual labor rate of government employee * locality factor) * FTE * duration in % of year * number of cores) * (1-FC NG911 Current Status%))

D.7.8.3. *National-level Cybersecurity Monitoring and Response*

There is a national-level coordinated cross-system cybersecurity program to respond to incidents. This national CERT, EC3, or IDPS will exist in the End State stage.

National-Level Cybersecurity Monitoring and Response Assumptions:
The cost of establishing a new monitoring function, or adding NG911 system monitoring to an existing monitoring and response function, is not known. Therefore, these costs were not included in the study.

D.8.   REFERENCE TABLES

D.8.1. GS SCHEDULE AND CONTRACTOR LABOR RATES

Table D-33 summarizes the General Schedule[115] loaded annual salaries (including benefits and fringe) for federal employees, as well annual salaries for four different levels of private contractors.

Table D-33: General Schedule Salary (September 2016) and Contractor Labor Rates

Grade/Category	Loaded Annual Salary
GS-1	$30,104
GS-2	$32,778
GS-3	$36,940
GS-4	$41,469
GS-5	$46,395
GS-6	$51,717
GS-7	$57,472
GS-8	$63,646
GS-9	$70,297
GS-10	$77,417
GS-11	$85,054

---

[115] "Pay & Leave," Office of Personnel Management, 2016, https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2016/general-schedule/.

Grade/Category	Loaded Annual Salary
GS-12	$101,947
GS-13	$121,231
GS-14	$143,255
GS-15	$168,510
CTR – Policy	$304,920
CTR – NetworkEng	$262,416
CTR – Telecom	$251,328
CTR – Emergency	$301,224

D.8.2. LOCALITY FACTOR TABLE

Table D-34 summarizes the locality factors[116] used to adjust federal and contractor annual salaries for each state.

Table D-34: Locality Factors

ID	Location	Locality Factor
ALB	Albany-Schenectady, NY	14.49%
ALQ	Albuquerque-Santa Fe-Las Vegas, NM	14.37%
ATL	Atlanta--Athens-Clarke County--Sandy Springs, GA-AL	19.58%
AUS	Austin-Round Rock, TX	14.51%
BOS	Boston-Worcester-Providence, MA-RI-NH-CT-ME	25.19%
COL	Columbus-Marion-Zanesville, OH	17.41%
DEN	Denver-Aurora, CO	22.93%
HAB	Harrisburg-Lebanon, PA	14.47%
HAR	Hartford-West Hartford, CT-MA	26.20%
IND	Indianapolis-Carmel-Muncie, IN	14.92%
MSP	Minneapolis-St. Paul, MN-WI	21.30%
NY	New York-Newark, NY-NJ-CT-PA	29.20%
PHL	Philadelphia-Reading-Camden, PA-NJ-DE-MD	22.22%
PX	Phoenix-Mesa-Scottsdale, AZ	17.12%
POR	Portland-Vancouver-Salem, OR-WA	20.69%
RA	Raleigh-Durham-Chapel Hill, NC	17.94%
RCH	Richmond, VA	16.76%

---

[116] "General Schedule (GS) Locality Pay Map," FederalPay.org, https://www.federalpay.org/gs/locality.

ID	Location	Locality Factor
SAC	Sacramento-Roseville, CA-NV	22.61%
AK	State of Alaska	25.16%
HI	State of Hawaii	16.81%
DCB	Washington-Baltimore-Arlington, DC-MD-VA-WV-PA	24.78%
RUS	Rest of United States	14.35%

D.8.3. COST ELEMENT STRUCTURE

Table D-35 summarizes the Cost Element Structure (CES) used in this cost study. Several elements are in place across multiple stages; the CES describes the stage in which each element is applied in the cost model. The CES is created using the maturity model domains, functional component, and elements.

Table D-35: Cost Element Structure

Description	Maturity Stage
Business Domain	
Planning	
Statewide NG911 Plan	Foundational
NG911 Concept of Operations	Transitional
Annually Review and Update Statewide NG911 Plan	End State
Governance	
Governance Gap Analysis	Foundational
Governance Plan	Foundational
Annually Review Governance Plan	End State
Policy	
Policy Gap Analysis	Foundational
Polices	Foundational
National Governance	
National Governance Gap Analysis	Foundational
National Governance Plan	Foundational
Regularly Review National Governance Plan	End State
Procurement	
Implementation	
Statewide Implementation Coordination	Foundational
Implementation Project Management	Foundational
Data Domain	
Geographic Information Systems Data	

Description	Maturity Stage
Local or No Data	Legacy
Developing Regional and Statewide Datasets	Foundational
GIS for Location Verification	Transitional
Maintain Developed Statewide Dataset	Intermediate
GIS for Routing	Intermediate
National GIS Data Set	End State
Location Data	
Traditional ALI	Legacy
Location Database (LDB)	Intermediate
Location Information Server (LIS)	End State
Additional Data	
Silo and Proprietary Data	Legacy
Shared Standard-based Data	Intermediate
System Control and Management Data	
Silo and Proprietary Data	Legacy
Shared Standard-based Data	Intermediate
Applications and Systems Domain	
Call Routing	
Trunk or Selective Routing	Legacy
IP Selective Routing	Foundational
Geospatial Routing with Traditional Rules	Intermediate
Geospatial Routing with Progressive Rules	End State
Call Handling Systems	
Legacy CPE	Legacy
IP-based Call Handling Systems	Intermediate
Location Validation	
MSAG Validation	Legacy
Geospatial Validation	Intermediate
Location Delivery	
Post Call Delivery over Dedicated ALI Circuits	Legacy
Post Call Delivery over Dedicated IP Circuits	Foundational
Delivery over IP Circuits	Transitional
Delivery by PIDF-LO in SIP header	Intermediate
Call Processing	
Silo and Proprietary Systems	Legacy
Standards-based systems	Intermediate
Event Logging	
Silo and Proprietary in Separate Systems	Legacy

Description	Maturity Stage
End-to-end Integrated Logging	Intermediate
Data Analysis	
Automated Data Analytics	Intermediate
Forest Guide	
Forest Guide in Place	Intermediate
National-level Forest Guide in Place	End State
Infrastructure Domain	
Data Centers	
Gateway Data Centers	Foundational
Core Data Centers	Foundational
Ingress Network	
TDM Connectivity	Legacy
Selective Router to NG911 Gateway	Foundational
Direct Connection to NG911 Gateway	Intermediate
Direct SIP Connections	End State
Egress Network	
TDM Connectivity	Legacy
Legacy PSAP Gateway	Foundational
PSAP Direct/Outbound Gateways	Transitional
Direct Connection via SIP	Intermediate
ESInet	
Dedicated Network for PSAPs	Foundational
Interconnected Networks	Intermediate
Nationwide ESInet	End State
Network Operations Center	
NOC Network Monitoring	Foundational
National-level NOC	End State
Non-voice Requests for Service	
Silo and Proprietary Systems	Legacy
Shared Standard-based Connections	Intermediate
Network-to-Network Interface	
Limited Interconnection	Foundational
Regional Interconnections	Intermediate
Seamless Interconnection	End State
PSAP-to-Responder Network	
Silo and Proprietary Systems	Legacy
Shared Standard-Based System	Intermediate
Security Domain	

Description	Maturity Stage
Border Control Function	
BCF Available and Functioning	Transitional
Facility and Personnel Security	
Individual System Log-in	Legacy
Local, Regional, or Statewide Single Log-in	Foundational
Trustmark Access	End State
Network and Security Monitoring	
Monitoring, Incident Management and Response	Foundational
Emergency Communications Cybersecurity Centers (EC3)	Intermediate
Operation/Performance Domain	
PSAP Training	
Develop, Implement, and Update PSAP Training	Foundational
Operational Procedures	
Develop, Implement, and Update Operational Procedures	Foundational
Managed Services	
Develop, Implement, and Maintain Managed Services	Foundational
Service Level Agreements	
Develop, Implement, and Maintain SLAs	Foundational
Contingency Plans	
Develop, Implement, and Update Contingency Plans	Foundational
Data Quality Assurance and Analysis	
Develop, Implement, and Update Data QA	Foundational
System Testing	
Develop, Implement, and Maintain System Testing	Foundational
Cybersecurity Program	
Multiple Diverse Cybersecurity Programs	Foundational
Coordinated Cross-system Cybersecurity Program	Intermediate
National-level Cybersecurity Monitoring and Response	End State

D.8.4. REGIONAL DATA TABLE

Table D-36: Regional Data

State	FEMA Region	2010 Census, Federal Highways Administration (FHWA)				2016 National 911 Progress Report		FCC's *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*		FCC *Voice Telephone Services* report (2015)			
Source:	FEMA	Population	Population per sq. miles	Total Area (Sq. Miles)	# of Counties	Primary PSAPs	Secondary PSAPs	Primary PSAPs	Secondary PSAPs	Wireline Service Providers	Switch Access Providers	VoIP Service Providers	Mobile Service Provider
Alabama	4	4,779,736	94	52,419	67	143	8	118	0	175	61	145	7
Alaska	10	710,231	1	663,267	30	95	3	38	5	65	18	49	12
Arizona	9	6,392,017	56	113,998	15	106	13	76	10	189	51	165	7
Arkansas	6	2,915,918	56	53,179	75	105	17	102	29	135	48	101	4
California	9	37,253,956	239	163,696	58	434	61	399	51	297	83	260	6
Colorado	8	5,029,196	49	104,094	64	94	10	91	8	225	67	186	11
Connecticut	1	3,574,097	738	5,543	8	110	11	110	0	163	40	147	4
Delaware	3	897,934	461	2,489	3	9	0	8	1	107	29	94	4
District of Columbia	3	601,723	9,857	68	1	5	1	1	0	131	33	117	4
Florida	4	18,801,310	351	65,755	67	222	34	154	52	287	81	244	6
Georgia	4	9,687,653	168	59,425	159	185	22	135	23	243	89	198	5
Hawaii	9	1,360,301	212	10,931	5	7	3	5	3	55	9	52	5
Idaho	10	1,567,582	19	83,570	44	48	22	46	2	130	43	110	10
Illinois	5	12,830,632	231	57,914	102	340	30	253	25	283	107	224	9
Indiana	5	6,483,802	181	36,418	92	163	10	91	28	206	79	163	5
Iowa	7	3,046,355	55	56,272	99	112	13	114	0	265	184	113	61
Kansas	7	2,853,118	35	82,277	105	147	1	117	0	188	78	135	9
Kentucky	4	4,339,367	110	40,409	120	166	15	115	40	154	56	129	7
Louisiana	6	4,533,372	105	51,840	64	106	3	57	50	158	46	136	6
Maine	1	1,328,361	43	35,385	16	27	0	26	0	98	36	82	5
Maryland	3	5,773,552	595	12,407	24	31	10	24	52	193	57	170	6
Massachusetts	1	6,547,629	839	10,555	14	254	2	249	81	185	50	167	4
Michigan	5	9,883,640	175	96,716	83	154	44	145	0	211	72	179	6
Minnesota	5	5,303,925	67	86,939	87	99	19	99	5	203	96	141	6
Mississippi	4	2,967,297	63	48,430	82	147	2	103	30	134	44	111	6
Missouri	7	5,988,927	87	69,704	115	176	14	0	0	203	72	160	8
Montana	8	989,415	7	147,042	56	59	1	53	0	102	38	77	7
Nebraska	7	1,826,341	24	77,354	93	82	9	71	0	141	61	98	8
Nevada	9	2,700,551	25	110,561	17	28	10	12	3	151	46	129	6
New Hampshire	1	1,316,470	147	9,350	10	6	0	2	0	121	37	107	5
New Jersey	2	8,791,894	1,196	8,721	21	187	7	0	0	205	63	183	4
New Mexico	6	2,059,179	17	121,589	33	91	0	45	2	127	40	110	9

Source:	FEMA	2010 Census, Federal Highways Administration (FHWA)				2016 National 911 Progress Report		FCC's *Eighth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*		FCC *Voice Telephone Services* report (2015)			
State	FEMA Region	Population	Population per sq. miles	Total Area (Sq. Miles)	# of Counties	Primary PSAPs	Secondary PSAPs	Primary PSAPs	Secondary PSAPs	Wireline Service Providers	Switch Access Providers	VoIP Service Providers	Mobile Service Provider
New York	2	19,378,102	411	54,556	62	193	5	134	51	268	91	228	5
North Carolina	4	9,535,483	196	53,819	100	135	21	119	6	227	63	197	7
North Dakota	8	672,591	10	70,700	53	22	8	22	0	108	49	73	7
Ohio	5	11,536,504	282	44,825	88	342	1	143	60	233	91	183	5
Oklahoma	6	3,751,351	55	69,898	77	177	0	133	0	172	71	124	12
Oregon	10	3,831,074	40	98,381	36	49	37	43	14	179	69	143	6
Pennsylvania	3	12,702,379	284	46,055	67	86	2	69	0	240	78	203	10
Rhode Island	1	1,052,567	1,018	1,545	5	71	0	1	0	100	27	90	4
South Carolina	4	4,625,364	154	32,020	46	81	12	77	0	162	52	140	6
South Dakota	8	814,180	11	77,117	66	33	0	29	0	115	55	79	8
Tennessee	4	6,346,105	154	42,143	95	161	13	140	30	203	64	169	7
Texas	6	25,145,561	96	268,581	254	590	37	490	64	348	123	276	12
Utah	8	2,763,885	34	84,899	29	44	0	32	4	148	42	128	8
Vermont	1	625,741	68	9,614	14	6	0	6	0	89	31	75	5
Virginia	3	8,001,024	203	42,774	133	143	24	121	40	207	58	183	7
Washington	10	6,724,540	101	71,300	39	72	52	54	9	198	66	167	6
West Virginia	3	1,852,994	77	24,230	55	53	8	52	0	119	36	98	8
Wisconsin	5	5,686,986	105	65,498	72	143	1	139	0	190	82	133	9
Wyoming	8	563,626	6	97,814	23	53	0	0	0	99	32	81	9
Puerto Rico	2	3,725,789	1,088	5,325	78	1	0	2	0	22	6	20	5
Guam	9	159,358	770	210	19	3	0	0	0	2	1	1	4
U.S. Virgin Islands	2	106,405	100	133	3	2	0	2	0	5	1	4	4
American Samoa	9	55,519	695	76	3	1	0	1	0				
Northern Mariana Islands	9	53,883	262	179	1	0	0	0	0	1	1		2

APPENDIX E – COST ANALYSIS DETAILED RESULTS

The analysis focused on the most defensible implementation alternatives to provide a cost estimate of planning, acquisition, implementation, and sustaining Next Generation 911 (NG911) systems for the entire United States (U.S.), including territories. The cost study leveraged an evaluation of current environment (i.e., Maturity Model NG911 current status) as well as a series of actual and estimated cost data from publicly and privately available sources. The analysis is most useful in gaining an understanding of the actual cost categories required for each functional component within the maturity model, as well as a nationwide-level estimate based on the assumptions. Thus, while the estimates of total cost are dependent on the assumptions of projected implementation scenarios, and as such are uncertain (due to inherent uncertainty in any long-term predictions), all global assumptions are held constant for all Federal Emergency Management Agency (FEMA) regions. Therefore, by holding the global assumptions constant, it was possible to introduce state-level inputs and assumptions into the multistate areas and create unique and meaningful estimates.

The aggregation of regional estimates, as well as nationwide-level cost requirements, resulted in total ten-year costs of NG911 systems presented here. As a result, the analysis is most credible when viewed as the total nationwide NG911 cost, and is not intended to help determine individual state or locality costs. The uncertainty analysis shows that with the cost-driving inputs, most of the uncertainty lies to the downside (i.e., quantities of public safety answering points [PSAPs], numbers of existing originating service providers [OSPs], and industry equipment prices). Therefore, the current estimate still represents a conservative estimate.

It is important to note the aspects below that must be considered as the nationwide results are evaluated.

- The results include NG911 costs to achieve the End State for every area that is not yet expended or planned.
- The results exclude costs that an area has expended or is currently operating as components of an evolving, NG911-capable implementation.
- Any future technology enhancements and/or economy-of-scale applications can change the results drastically.
- Deviations from any of the implementation scenarios presented in this report can change the total cost.
- Actual start year and implementation path chosen by each area also can result in deviations from the total ten-year lifecycle cost estimate.

E.1.   IMPLEMENTATION SCENARIOS

The results shown in this appendix represent a slightly different view of the cost analysis. The charts and figures depicted within represent the total ten-year lifecycle cost of the various implementation scenarios including the needed maintenance and equipment refresh costs during the period. The main body of the report only includes the deployment and transition costs, excluding costs after the second year of operation for areas where the NG911 implementation may be completed quickly. Additionally, the main body excludes the cost of equipment refreshes for that which may be necessary within ten years. These costs are included within this appendix.

E.1.1. STATE IMPLEMENTATION SCENARIO RESULTS

Figure E-1 depicts the NG911 total ten-year nationwide cost by allocation for the state implementation scenario. Approximately one-third of the total ten-year cost is allocated to NG911 core services and another one-third to PSAPs. The remaining cost is allocated to OSPs, state, and federal categories.
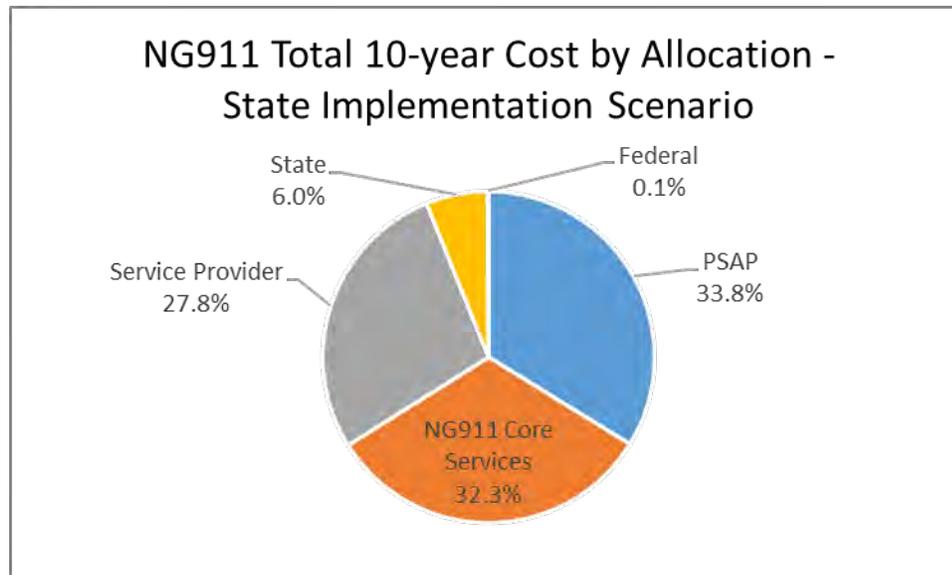
Figure E-1: NG911 Total Ten-year Cost Allocation – State Implementation Scenario

Figure E-2 summarizes the breakdown of the NG911 total ten-year cost by domain for the state implementation scenario. The majority of hardware, software, and services required for implementing the NG911 End State is captured under the Applications and Systems Domain (lighter blue). As more states implement NG911 systems, the total annual costs increase. Also, any end-of-life refresh and ongoing maintenance required for the equipment is captured in the Applications and Systems Domain and accounts for the bulk of this value.
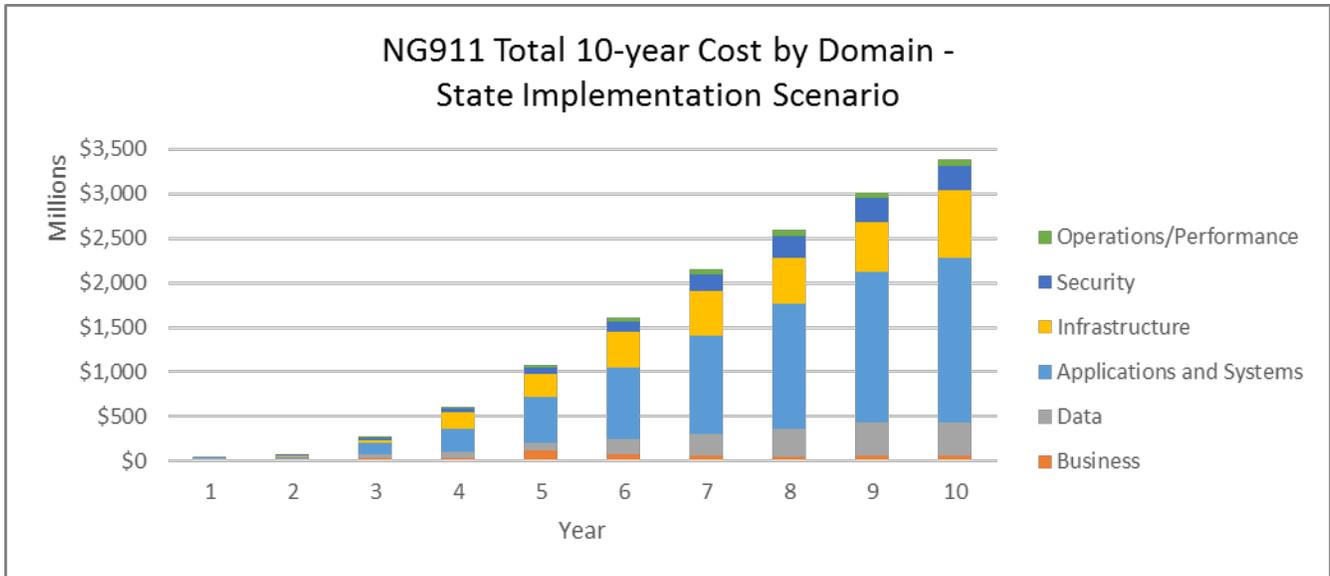
Figure E-2: NG911 Total Ten-year Cost by Domain – State Implementation Scenario

Infrastructure is the second-largest cost category (yellow), as shown in Figure E-2, and accounts for all connectivity and bandwidth costs needed for the NG911 End State. Again, as more states advance in their NG911 systems deployment, these costs increase. The last year of the analysis should be generally flat into the next few years after the analysis, then decline slightly. Assuming a future optimal maintenance strategy, thereafter should remain steady (plus some accounting for inflation).

Figure E-3 below shows the total ten-year cost of NG911 for the state implementation scenario by FEMA regions. It is important to recognize that this cost breakdown is based on the current status of states within each region, as well as their individual unique geographical requirements in achieving the end state. Specific characteristics of each region, in addition to an assessment of their NG911 deployment readiness, has resulted in the following total ten-year cost:
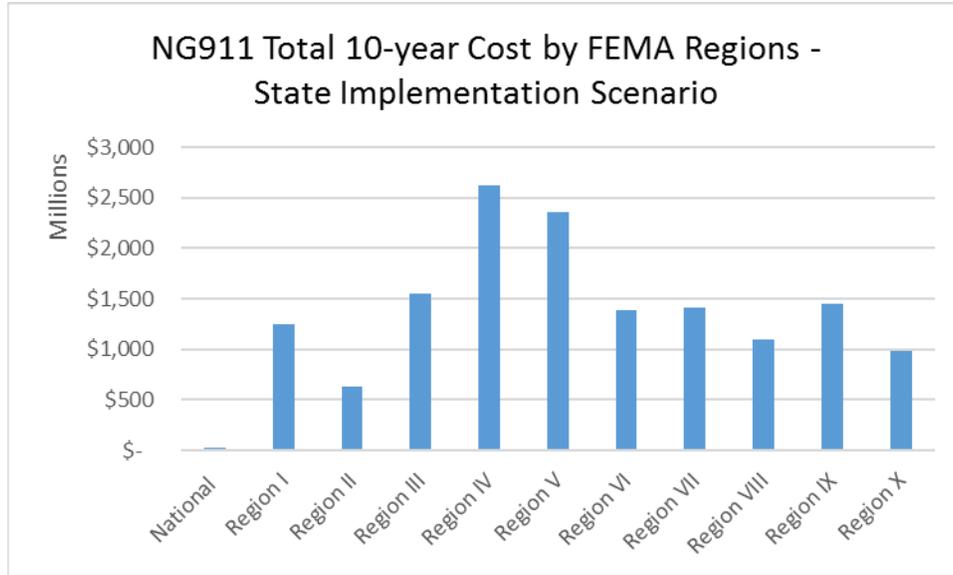
Figure E-3: NG911 Total Ten-year Cost by Region – State Implementation Scenario

E.1.2. MULTISTATE IMPLEMENTATION SCENARIO RESULTS

Figure E-4 summarizes the total ten-year NG911 nationwide cost by allocation for the multistate implementation scenario. This scenario assumes two mega-sized NG911 cores for each multistate area, and compared with the individual state implementation scenario, the NG911 core services cost allocation is less. PSAP cost allocation accounts for the largest portion of this scenario. The remaining cost is allocated to the OSP, state, and federal categories.
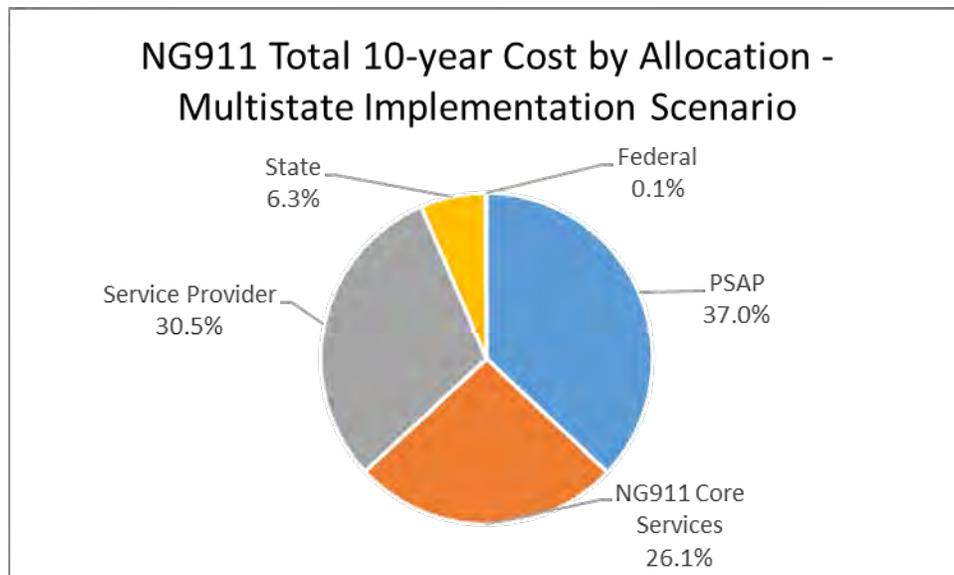
Figure E-4: NG911 Total Ten-year Cost Allocation – Multistate Implementation Scenario

Figure E-5 summarizes the breakdown of the NG911 total ten-year cost by domain for the multistate implementation scenario. Similar to the individual state implementation scenario, the largest category of cost is accounted for in the Applications and Systems Domain (lighter blue), which captures most of the hardware, software, and services required for implementing the NG911 End State. As more states implement NG911 systems, the total annual costs increase. Also, any end-of-life refresh and ongoing maintenance required for the equipment is captured in the Applications and Systems Domain and accounts for the bulk of this value.
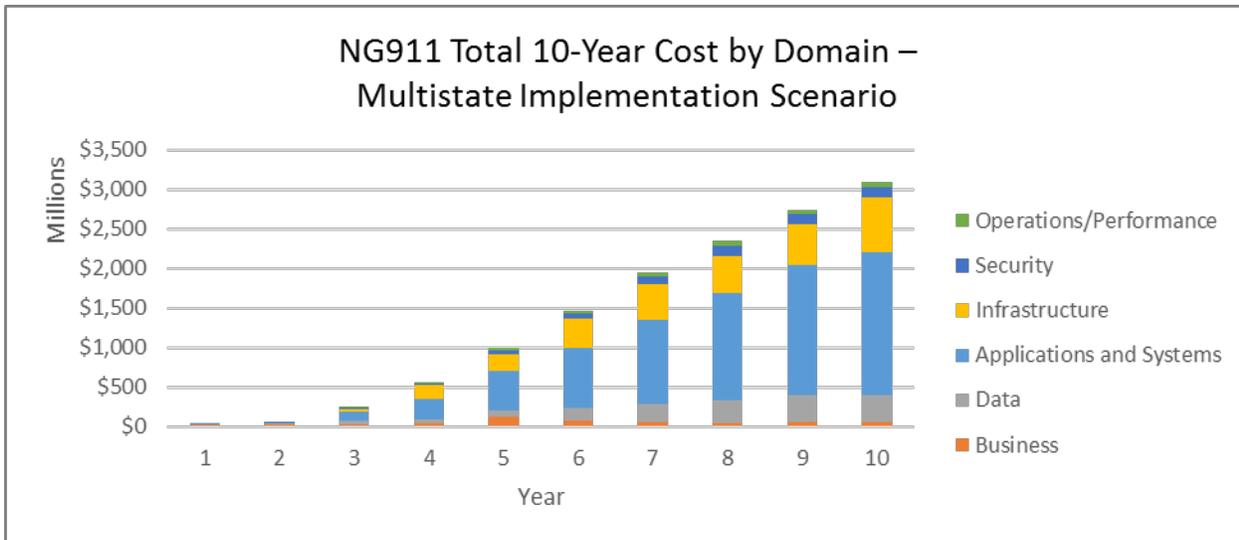
Figure E-5: NG911 Total Ten-year Cost by Domain – Multistate Implementation Scenario

Infrastructure is the second-largest cost category (yellow), as shown in Figure E-5, and accounts for all connectivity and bandwidth costs needed for the NG911 End State. Again, as more states advance in their NG911 systems deployment, these costs increase.

Figure E-6 below shows the total ten-year cost of NG911 for the multistate implementation scenario by FEMA regions. These results demonstrate the cost of deploying two mega Next Generation Core Services (NGCS) within each region, in addition to small core systems at the geographically isolated locations. Depending on the readiness of each state within a region and the region's unique characteristics and requirements, the costs of total NG911 deployment vary between different regions.
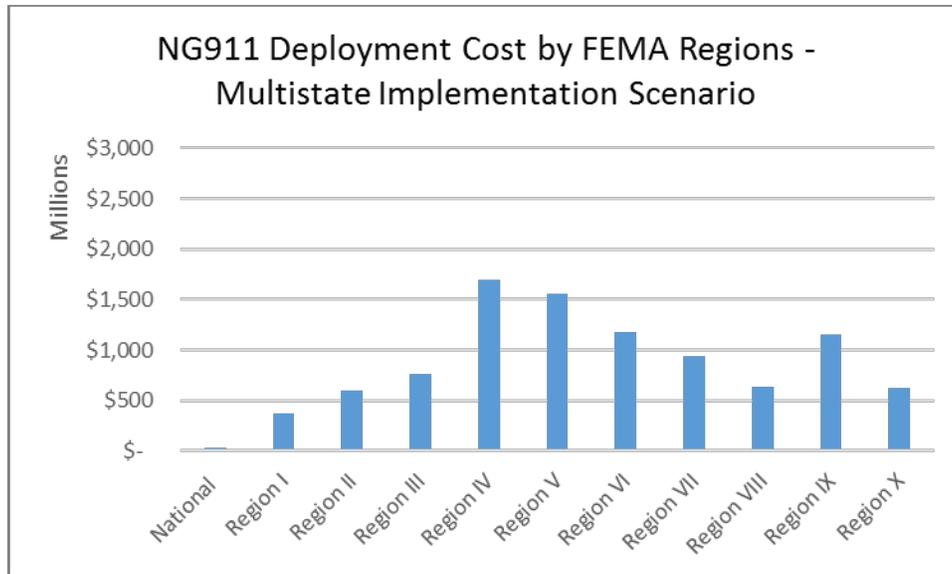
Figure E-6: NG911 Total Ten-year Cost by Region – Multistate Implementation Scenario

E.1.3. SERVICE SOLUTION SCENARIO RESULTS

For the service solution scenario, it is assumed that core services from major service providers would be utilized for every state. As stated earlier, this option is architecturally similar to the multistate implementation scenario and, therefore, that scenario is utilized as a proxy for the costs that service providers incur to generate viable NG911 services. All core services and capability at the PSAPs are, instead, provided by a service provider. The costs for services from the multistate implementation scenario were used as the starting point for this alternative, and were cross-checked with data received from some vendors for the applicable elements of this scenario. As this is not a pricing verification or realism analysis of any specific vendor, the only conclusion is that this appears to correlate with the service costs that the states may pay. While this option smooths spikes in a state's expenditure, it was not verified that these prices will stay the same for all states, and may fluctuate between them.

For purposes of the analysis, the costs are broken down into three categories: annualized investment and refresh service costs, annualized operations service costs, and annualized non-service costs. The annualized investment and refresh service costs represent the initial acquisition and maintenance costs of PSAPs and NG911 core services through a hosted solution. The annualized operations service costs represent the ongoing operations and maintenance costs of PSAPs and NG911 core services. The final category of annualized non-service costs represents all additional costs allocated to service providers, state, and federal entities; similar to those contained within the multistate implementation scenario.

Figure E-7 summarizes the total ten-year NG911 cost for the service solution scenario. The annualized service costs presented are susceptible to market forces of any individual vendor's approach for bidding to be a state provider. This scenario has the largest ten-year cost. An analysis would be expected for a state to decide whether the benefits to them outweigh what was proposed, as they could possibly even save money over ten years depending on market conditions in their circumstance.
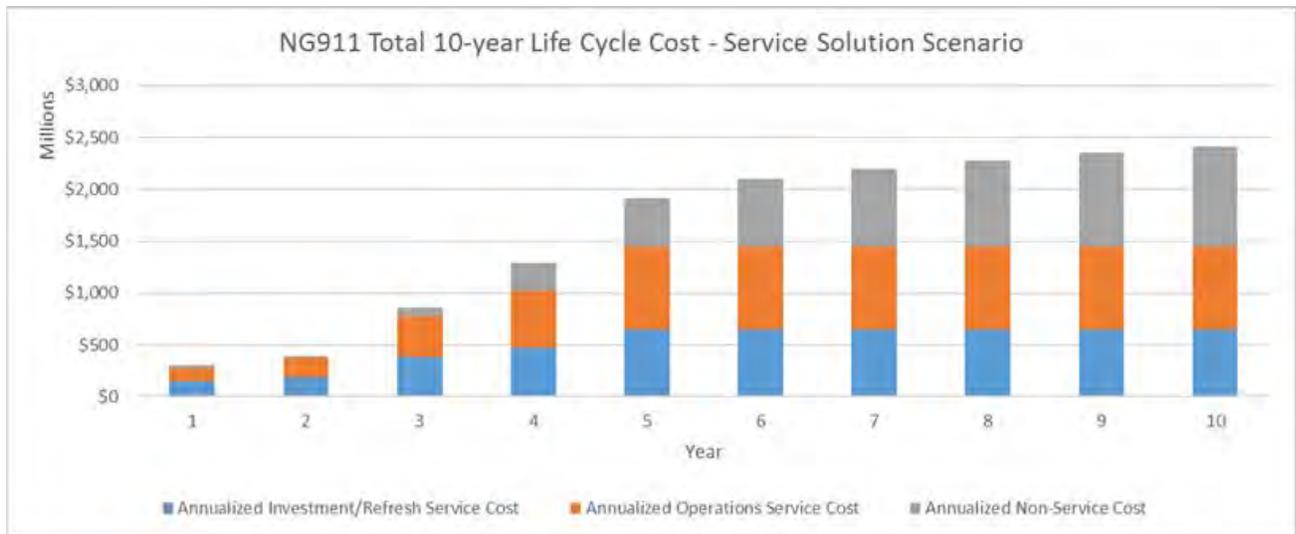
Figure E-7: NG911 Total Ten-year Lifecycle Cost – Service Solution Scenario

E.2.   UNCERTAINTY ANALYSIS

Several variables had a significant impact on the estimation and were recognized as cost drivers. The major cost drivers identified for this analysis were:
- Number of NG911 core systems fielded
- Number of PSAP call-taker positions
- Government or contractor level of effort to conduct the various functions
- Quantity and size of communication bandwidth connections necessary between NG911 nodes
- Cost examples collected from industry
- Subject-matter expert (SME) inputs.

The minimum and maximum values assigned to each cost driver were based on engineering judgment, industry standards, and SME input.

Uncertainty analysis was conducted on the total cost estimate for the state implementation and multistate implementation scenarios to understand the calculated confidence levels. The cost drivers in the model were assigned a range of values (separately for quantities and unit costs) and then the Monte Carlo Analysis was conducted to assess their contributions to the variations in the calculation result. Values for the cost drivers were selected between the minimum and maximum values in a triangular distribution around the most likely value. Ten thousand Monte Carlo iterations were run and the output was analyzed to understand the impact upon the scenario results.

Figure E-8 summarizes the results of the Monte Carlo Analysis for the state implementation scenario. As reported earlier, the total NG911 ten-year cost estimate for this scenario is approximately $14.8 billion. This number corresponds to roughly the 86 percent confidence interval on the graph. Estimated values for 30, 50, 80, and 90 percent confidence intervals are presented on the graph as well.
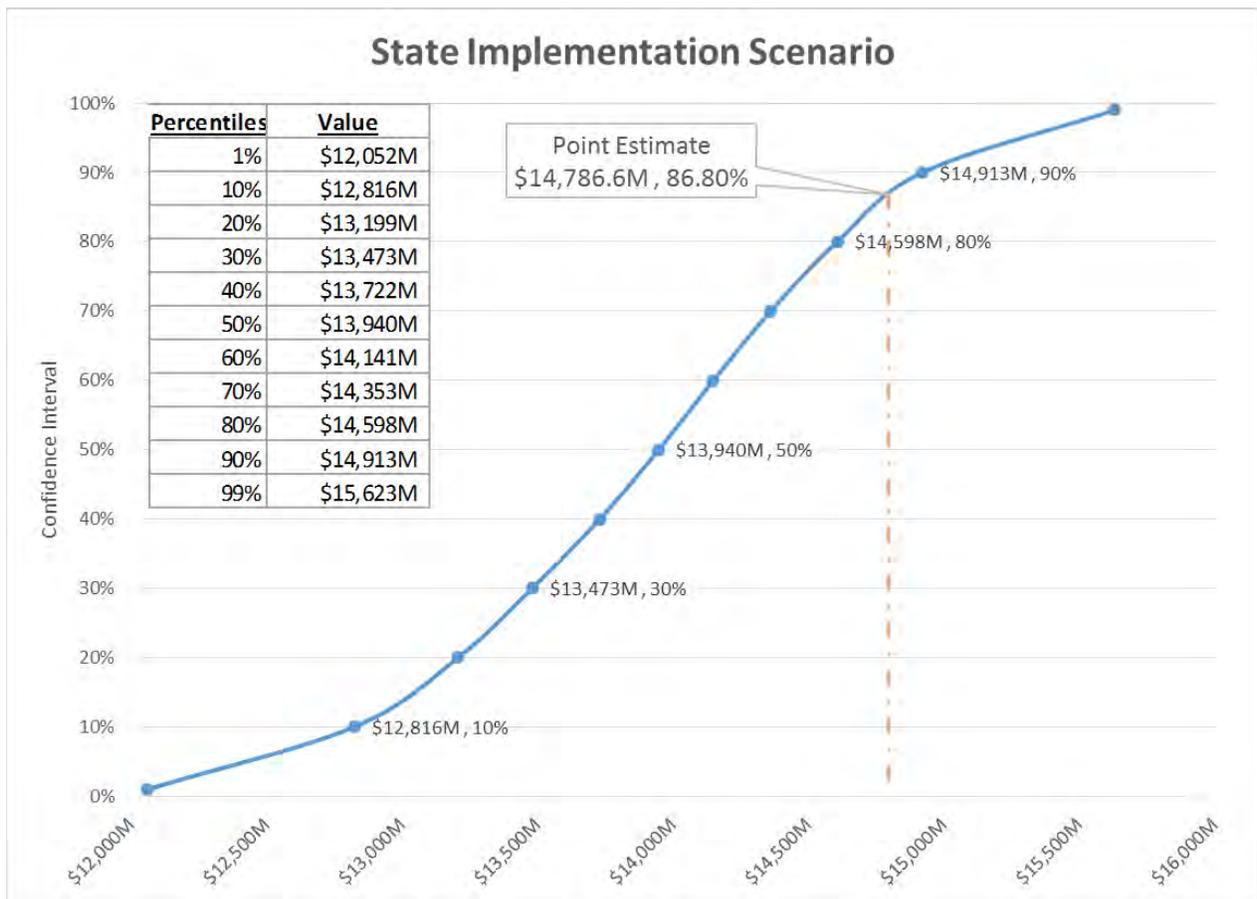
Figure E-8: NG911 Total Ten-year Cost – State Implementation Scenario

Similarly, Figure E-9 summarizes the results of the Monte Carlo Analysis for the multistate implementation scenario. As reported earlier, the total NG911 ten-year cost estimate for this

scenario is approximately $13.5 billion. This number corresponds to roughly the 87 percent confidence interval on the graph.

Multistate Implementation Scenario

Percentiles	Values
1%	$10,928M
10%	$11,643M
20%	$11,996M
30%	$12,253M
40%	$12,481M
50%	$12,683M
60%	$12,873M
70%	$13,069M
80%	$13,304M
90%	$13,599M
99%	$14,248M

Point Estimate
$13,494.2M , 86.90%
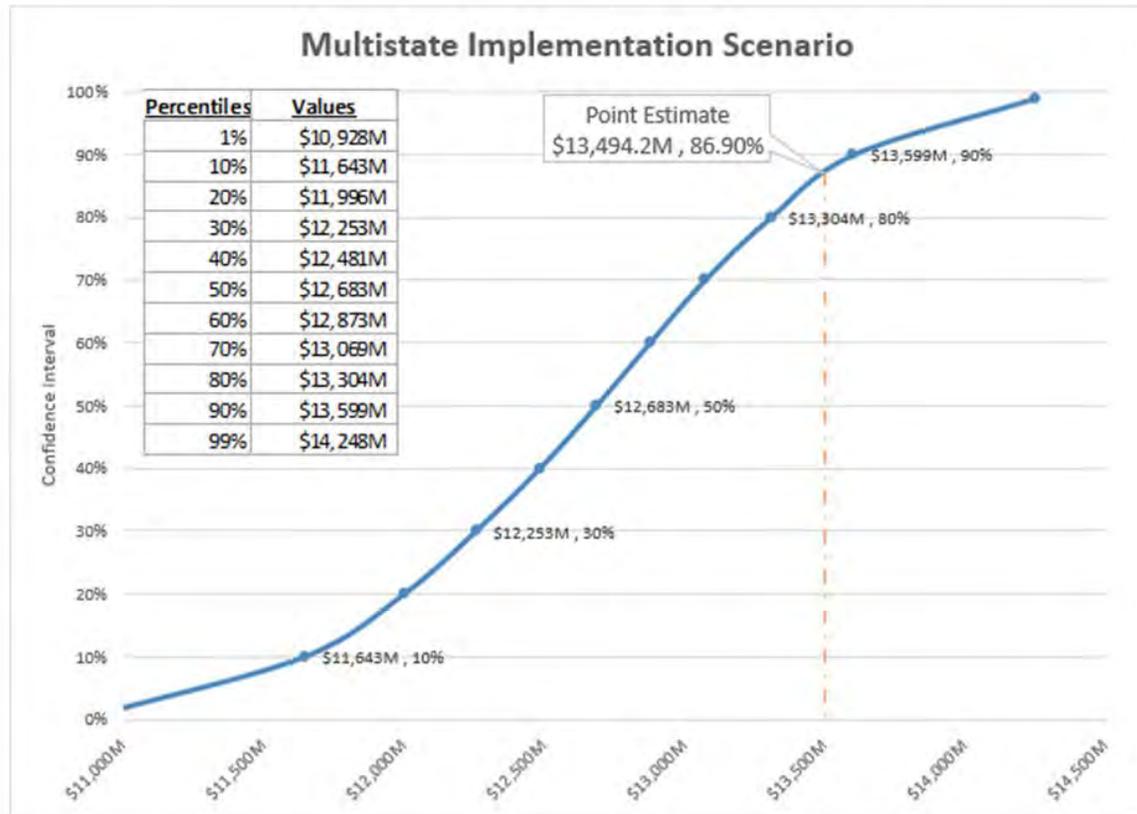
Figure E-9: NG911 Total Ten-year Cost – Multistate Implementation Scenario

As both the state and multistate implementation cost estimates represent relatively high confidence levels for the complete estimate, these respective costs have been used to represent the complete cost of NG911 throughout the entire document, instead of ranges.

E.2.1. TOTAL TEN-YEAR LIFECYCLE COST VERSUS DEPLOYMENT COST EXCURSION

While the goal of the analysis was to gain an understanding of and determine the costs of a ten-year lifecycle for each scenario, it is important to recognize that there is another way to examine the costs. Acknowledging that some states are at different points of their NG911 implementation schedules means that they will complete on different timelines.

As the desired End State is achieved, there is expected to be some time where the system must operate to complete a break-in period and to retire legacy systems. After this period, states are expected to continue operating and maintaining their expected NG911 functionality. The charts

and tables in this section depict the complete lifecycle costs, but end with the second year after an area has reached its End State, and exclude any equipment refresh costs. As with the primary scenarios, these deployment cost excursions include the complete costs to include acquisition, implementation and operation of the NG911 capabilities not already in place.

The body of this document exclusively presents results of the three deployment cost scenarios, and a summary is shown again in Table E-1.

Table E-1: NG911 Total Deployment Cost Estimation

Cost Type	State Implementation	Multistate Implementation	Service Solution
One-Time Cost	$3,022.3M	$2,898.8M	$599.3M
Recurring Cost	$7,508.1M	$6,606.5M	$12,115.3M
Total	**$10,530.4M**	**$9,505.3M**	**$12,714.6M**

Figure E-10 shows the year-by-year costs of these deployment excursions for the three implementation scenarios. For the state and multistate scenarios, costs begin to decrease in years 8 and 9 as early-adopting regions and fast implementers have surpassed their End State by two years; the increases in year 10 represent the slow-adopting regions just reaching their first full year of operation. Meanwhile, the service solution shows a steady increase as regions begin, and decreases as the End State is achieved.
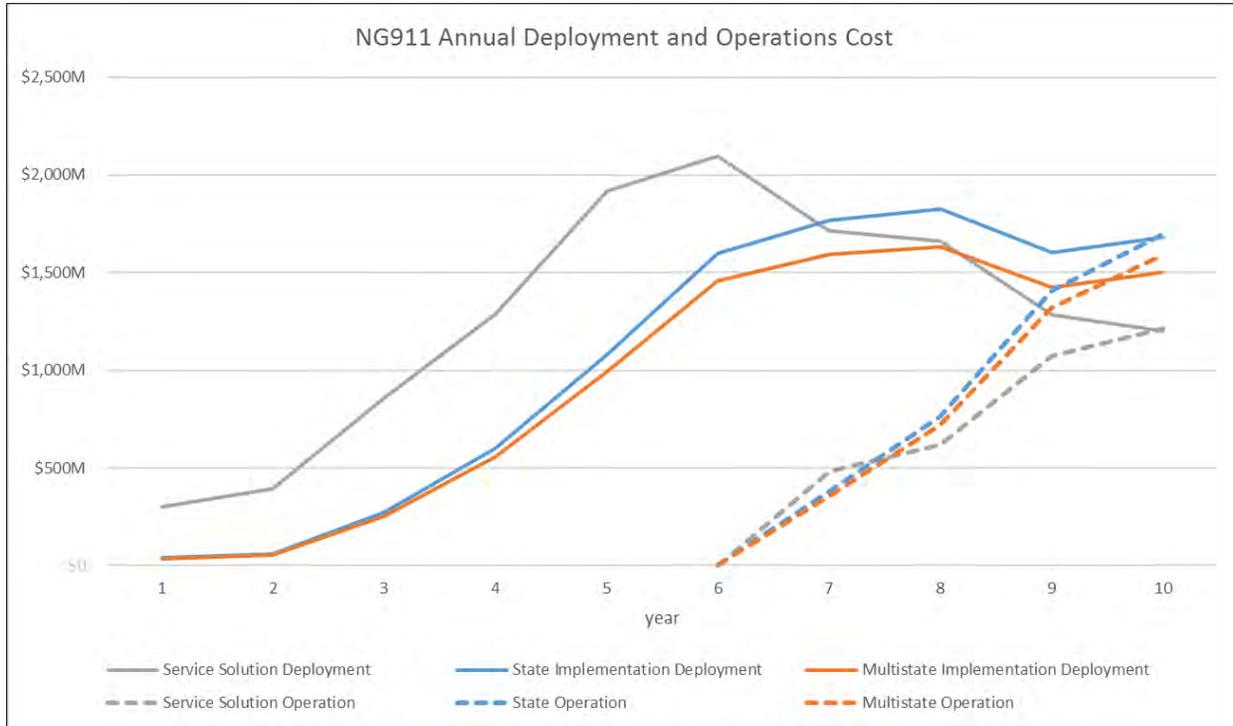
Figure E-10: NG911 Annual Deployment and Operations Cost

E.2.2. COST ANALYSIS SUMMARY

The scenarios in this total cost analysis are built at the regional level using the maturity model, cost assumptions and details discussed in this report. Using that information, for each scenario, the total ten-year lifecycle costs are shown in Table E-2.

Table E-2: NG911 Total Ten-Year Lifecycle Cost Estimation

Cost Type	State Implementation	Multistate Implementation	Service Solution
One-Time Cost	$3,023.1M	$2,899.5M	$600.1M
Recurring Cost	$10,716.7M	$9,603.5M	$15,502.2M
Refresh	$1,046.8M	$991.2M	$0
Total	**$14,786.6M**	**$13,494.2M**	**$16,102.3M**

As expected, if states adopt the multistate implementation scenario, there will be a savings in the NG911 core services of almost $1.3 billion across the ten years. Under the service solution model, the lifecycle costs would be larger, but each state would experience a steady cost that is more predictable. The states also may benefit from competition within the NG911 marketplace, which

could create more flexibility over time. However, it is not yet clear that the prices currently in place by the vendors are those that will be experienced by the states over the long term. With the current assumptions, the service solution scenario would cost an additional $1.3 billion compared with the state implementation scenario.

In the deployment-only analysis, all scenario costs are decreased as operational and equipment replacements are removed. The overall premium paid out in the service solution scenario is almost $2.2 billion greater than the state implementation, as shown in Table E-3. For the primary implementation scenarios, equipment refresh is removed outside of this deployment window. However, under the service solution scenario, the vendor is expected to maintain and upgrade all the equipment for the annual service price. This essentially includes this refresh cost back inside the deployment window, resulting in the larger value.

Table E-3: NG911 Total Deployment Cost Estimation

Cost Type	State Implementation	Multistate Implementation	Service Solution
One-Time Cost	$3,022.3M	$2,898.8M	$599.3M
Recurring Cost	$7,508.1M	$6,606.5M	$12,115.3M
Total	**$10,530.4M**	**$9,505.3M**	**$12,714.6M**

It must be noted that while each scenario assumes that the entire country will utilize a homogeneous path forward, it is expected that with federal and state budget and planning realities, this is highly unlikely. Therefore, the specific path for each state or region, and the cost of the nationwide solution, will be some sort of combination of all alternatives.

Table E-4 summarizes the annual cost by functional component for the state implementation scenario.

Table E-5 summarizes the annual cost by functional component for the multistate implementation scenario.

Please note that these figures are rounded in the millions for simplicity. Thus, these figures do not necessarily add to the grand total due to the rounding factor.

Table E-4: Ten-year Annual Cost by Functional Component for the State Implementation Scenario

Cost Element Structure (Then-Year in $Millions)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total
Business	**$24.9**	**$21.4**	**$36.9**	**$38.8**	**$124.0**	**$78.6**	**$57.9**	**$49.1**	**$59.3**	**$63.8**	**$554.7**
Planning	$1.8	$7.3	$5.6	$7.1	$19.7	$23.0	$16.2	$1.9	$4.1	$4.2	$90.8
Governance	$8.5	$3.2	$7.3	$5.8	$30.1	$10.8	$2.7	$3.6	$7.1	$7.2	$86.2
Policy	$13.4	$9.0	$18.9	$16.6	$52.5	$20.3	$10.1	$10.3	$10.5	$10.7	$172.2
National Governance	$0	$0	$0	$0	$4.5	$1.5	$0.4	$0.4	$0.4	$0.4	$7.7
Procurement	$0.3	$0.4	$2.4	$5.6	$10.3	$15.2	$20.5	$24.7	$28.9	$32.8	$141.1
Implementation	$0.9	$1.5	$2.9	$3.9	$6.8	$7.8	$8.0	$8.1	$8.3	$8.4	$56.7
Data	**$12.0**	**$16.3**	**$34.4**	**$60.6**	**$86.2**	**$170.5**	**$244.0**	**$317.3**	**$374.0**	**$374.5**	**$1,689.9**
Geographic Information Systems Data	$12.0	$16.3	$33.1	$55.8	$75.6	$151.2	$214.2	$278.1	$328.2	$325.7	$1,490.2
Location Data	$0	$0	$1.3	$4.8	$10.7	$19.3	$29.8	$39.2	$45.7	$48.8	$199.6
Apps	**$2.9**	**$7.5**	**$127.4**	**$265.6**	**$517.2**	**$797.2**	**$1,109.9**	**$1,398.4**	**$1,689.9**	**$1,847.8**	**$7,763.7**
Call Routing	$2.9	$7.5	$22.3	$40.2	$54.9	$86.3	$110.6	$114.4	$118.3	$110.9	$668.2
Call Handling Systems	$0	$0	$37.1	$52.0	$146.4	$217.3	$356.4	$576.7	$839.8	$1,015.3	$3,241.1
Location Validation	$0	$0	$0.7	$1.2	$1.8	$2.4	$3.2	$3.2	$3.0	$1.9	$17.5
Location Delivery	$0	$0	$29.5	$103.3	$206.1	$330.0	$425.1	$470.3	$490.4	$499.6	$2,554.1
Call Processing	$0	$0	$5.6	$18.5	$34.8	$56.4	$84.0	$110.0	$128.8	$138.2	$576.3
Event Logging	$0	$0	$30.8	$48.4	$71.1	$102.4	$127.4	$120.3	$106.3	$79.6	$686.3
Data Analysis	$0	$0	$1.4	$1.9	$1.9	$2.3	$3.1	$3.3	$3.3	$2.2	$19.3
Forest Guide	$0	$0	$0.1	$0.1	$0.1	$0.1	$0.1	$0.2	$0.2	$0.1	$0.9
Infrastructure	**$0**	**$10.7**	**$38.1**	**$187.7**	**$250.3**	**$401.5**	**$503.0**	**$514.8**	**$562.0**	**$746.3**	**$3,214.4**
Data Centers	$0	$0.6	$2.5	$10.2	$20.7	$33.2	$47.1	$45.9	$39.5	$43.6	$243.2
Ingress Network	$0	$2.5	$15.0	$131.3	$145.9	$239.4	$241.7	$255.7	$303.9	$345.0	$1,680.4
Egress Network	$0	$2.0	$6.9	$16.7	$33.6	$54.7	$122.0	$135.0	$137.3	$269.6	$777.9

Cost Element Structure (Then-Year in $Millions)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total
ESInet	$0	$3.1	$6.3	$14.9	$29.2	$43.5	$57.2	$59.9	$64.5	$78.8	$357.5
Network Operations Center (NOC)	$0	$1.5	$3.1	$6.2	$11.2	$14.7	$14.3	$1.8	$1.7	$1.9	$56.4
Non-Voice Requests for Service	$0	$0	$0.9	$2.5	$3.7	$7.7	$10.5	$7.7	$6.0	$0	$39.0
Network-to-Network Interface	$0	$1.0	$3.5	$6.0	$5.9	$8.3	$10.1	$8.8	$9.1	$7.3	$60.0
Security	**$0**	**$4.7**	**$24.3**	**$32.0**	**$78.0**	**$118.8**	**$179.9**	**$243.8**	**$268.1**	**$282.3**	**$1,231.9**
Border Control Function (BCF)	$0	$0	$2.0	$8.2	$27.6	$52.3	$84.9	$123.4	$153.9	$162.6	$615.0
Facility and Personnel Security	$0	$4.0	$17.1	$8.1	$24.1	$23.6	$32.6	$31.8	$10.4	$17.6	$169.3
Network and Security Monitoring	$0	$0.8	$5.2	$15.7	$26.3	$42.9	$62.3	$88.6	$103.8	$102.0	$447.6
Ops	**$0**	**$0**	**$9.8**	**$17.7**	**$23.9**	**$35.6**	**$55.5**	**$66.3**	**$60.7**	**$62.6**	**$332.0**
PSAP Training	$0	$0	$0.7	$1.6	$2.6	$4.0	$5.9	$7.2	$7.3	$7.4	$36.7
Operational Procedures	$0	$0	$0.1	$0.2	$0.3	$0.4	$0.6	$0.7	$0.7	$0.7	$3.7
Service Level Agreements	$0	$0	$0.1	$0.3	$0.5	$0.8	$1.2	$1.4	$1.5	$1.5	$7.4
Contingency Plans	$0	$0	$7.7	$12.9	$16.7	$25.0	$40.6	$47.4	$40.3	$41.0	$231.6
Data QA	$0	$0	$0.1	$0.3	$0.5	$0.8	$1.2	$1.4	$1.5	$1.5	$7.4
System Testing	$0	$0	$0.4	$0.8	$1.2	$1.6	$2.3	$2.9	$2.9	$3.0	$15.1
Cybersecurity Program	$0	$0	$0.7	$1.5	$2.1	$2.9	$3.7	$5.2	$6.5	$7.5	$30.2
Cost Element Structure (Then-Year in $Millions)	**$39.7**	**$60.7**	**$270.9**	**$602.5**	**$1,079.6**	**$1,602.3**	**$2,150.2**	**$2,589.7**	**$3,013.8**	**$3,377.3**	**$14,786.6**

Please note that these figures are rounded in the millions for simplicity. Thus, these figures do not necessarily add to the grand total due to the rounding factor.

Table E-5: Ten-year Annual Cost by Functional Component for the Multistate Implementation Scenario

Cost Element Structure (Then-Year in $Millions)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total
Business	**$24.9**	**$21.3**	**$36.8**	**$38.4**	**$123.2**	**$77.3**	**$56.1**	**$47.0**	**$56.9**	**$61.3**	**$543.3**
Planning	$1.8	$7.3	$5.6	$7.1	$19.7	$23.0	$16.2	$1.9	$4.1	$4.2	$90.8
Governance	$8.5	$3.2	$7.3	$5.8	$30.1	$10.8	$2.7	$3.6	$7.1	$7.2	$86.2
Policy	$13.4	$9.0	$18.9	$16.6	$52.5	$20.3	$10.1	$10.3	$10.5	$10.7	$172.2
National Governance	$0	$0	$0	$0	$4.5	$1.5	$0.4	$0.4	$0.4	$0.4	$7.7
Procurement	$0.3	$0.4	$2.2	$5.2	$9.5	$13.9	$18.7	$22.6	$26.5	$30.3	$129.7
Implementation	$0.9	$1.5	$2.9	$3.9	$6.8	$7.8	$8.0	$8.1	$8.3	$8.4	$56.7
Data	**$12.0**	**$16.3**	**$34.1**	**$59.7**	**$83.0**	**$161.5**	**$227.4**	**$294.2**	**$347.1**	**$346.1**	**$1,581.3**
Geographic Information Systems Data	$12.0	$16.3	$33.0	$55.7	$75.5	$151.0	$214.0	$277.8	$327.9	$325.5	$1,488.7
Location Data	$0	$0	$1.1	$3.9	$7.5	$10.6	$13.4	$16.4	$19.1	$20.6	$92.6
Apps	**$1.4**	**$2.7**	**$117.9**	**$248.5**	**$492.4**	**$760.3**	**$1,062.2**	**$1,345.8**	**$1,636.1**	**$1,793.4**	**$7,460.7**
Call Routing	$1.4	$2.7	$13.3	$24.0	$31.8	$51.9	$66.3	$65.4	$67.9	$59.6	$384.2
Call Handling Systems	$0	$0	$37.1	$52.0	$146.4	$217.3	$356.4	$576.7	$839.7	$1,015.2	$3,240.9
Location Validation	$0	$0	$0.3	$0.6	$0.6	$0.6	$0.9	$1.0	$1.1	$0.6	$5.9
Location Delivery	$0	$0	$29.5	$103.3	$206.1	$330.0	$425.1	$470.3	$490.4	$499.6	$2,554.1
Call Processing	$0	$0	$5.6	$18.5	$34.8	$56.4	$84.0	$110.0	$128.8	$138.2	$576.3
Event Logging	$0	$0	$30.8	$48.4	$71.1	$102.4	$127.4	$120.3	$106.3	$79.6	$686.3
Data Analysis	$0	$0	$1.3	$1.7	$1.4	$1.5	$2.0	$2.0	$1.8	$0.6	$12.2
Forest Guide	$0	$0	$0.0	$0.1	$0.1	$0.0	$0.1	$0.1	$0.1	$0.1	$0.7
Infrastructure	**$0**	**$9.0**	**$34.0**	**$175.9**	**$225.6**	**$366.6**	**$460.6**	**$479.6**	**$527.7**	**$704.3**	**$2,983.1**
Data Centers	$0	$0.0	$0.7	$3.6	$7.6	$14.6	$22.7	$23.2	$18.2	$14.9	$105.6
Ingress Network	$0	$2.5	$15.0	$131.3	$145.9	$239.4	$241.7	$255.7	$303.9	$345.0	$1,680.4
Egress Network	$0	$2.0	$6.9	$16.7	$33.6	$54.7	$122.0	$135.0	$137.3	$269.6	$777.9
ESInet	$0	$3.0	$6.0	$13.6	$25.6	$36.3	$46.6	$47.8	$52.1	$66.2	$297.2

Cost Element Structure (Then-Year in $Millions)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total
Network Operations Center (NOC)	$0	$0.4	$1.0	$2.2	$3.3	$5.6	$6.8	$1.3	$1.1	$1.2	$23.0
Non-Voice Requests for Service	$0	$0	$0.9	$2.5	$3.7	$7.7	$10.5	$7.7	$6.0	$0	$39.0
Network-to-Network Interface	$0	$1.0	$3.5	$6.0	$5.9	$8.3	$10.1	$8.8	$9.1	$7.3	$60.0
Security	**$0**	**$4.1**	**$19.0**	**$17.2**	**$47.1**	**$63.2**	**$93.6**	**$122.2**	**$121.3**	**$129.3**	**$617.0**
Border Control Function (BCF)	$0	$0	$1.2	$5.0	$17.0	$29.3	$45.4	$66.1	$80.5	$82.7	$327.2
Facility and Personnel Security	$0	$3.9	$17.0	$8.0	$23.8	$23.2	$32.1	$31.3	$10.2	$17.1	$166.6
Network and Security Monitoring	$0	$0.1	$0.8	$4.2	$6.4	$10.6	$16.1	$24.8	$30.7	$29.5	$123.2
Ops	**$0**	**$0**	**$9.8**	**$17.7**	**$22.4**	**$31.0**	**$50.0**	**$62.2**	**$57.1**	**$58.9**	**$308.9**
PSAP Training	$0	$0	$0.7	$1.6	$2.4	$3.3	$4.6	$5.7	$5.8	$5.9	$30.1
Operational Procedures	$0	$0	$0.1	$0.2	$0.2	$0.3	$0.5	$0.6	$0.6	$0.6	$3.0
Service Level Agreements	$0	$0	$0.1	$0.3	$0.5	$0.7	$0.9	$1.1	$1.2	$1.2	$6.0
Contingency Plans	$0	$0	$7.7	$12.9	$15.5	$21.7	$37.6	$46.5	$40.3	$41.0	$223.2
Data QA	$0	$0	$0.1	$0.3	$0.5	$0.7	$0.9	$1.1	$1.2	$1.2	$6.0
System Testing	$0	$0	$0.4	$0.8	$1.2	$1.6	$2.3	$2.9	$2.9	$3.0	$15.1
Cybersecurity Program	$0	$0	$0.7	$1.5	$2.1	$2.8	$3.2	$4.2	$5.1	$5.9	$25.6
Grand Total (Then-Year in $Millions)	**$38.2**	**$53.4**	**$251.5**	**$557.3**	**$993.6**	**$1,459.9**	**$1,949.9**	**$2,350.9**	**$2,746.2**	**$3,093.3**	**$13,494.2**

APPENDIX F – REPORT AUTHORS

This report was completed under the United States Department of Transportation (DOT) National Highway Transportation Safety Administration (NHTSA) Task Order DTNH2215F00098 "Next Generation (NG) 911 Cost Study" by the Mission Critical Partners team of Mission Critical Partners, Inc. and Booz Allen Hamilton.

Mission Critical Partners (MCP) is a professional services firm that helps public safety clients enhance and evolve their mission-critical systems and operations. Through our breadth and depth of experience and an extensive network of resources, we are able to offer unique and successful solutions that solve our clients' complex challenges. Our planning, implementation and lifecycle management services span all aspects of mission-critical communications, while our expertise covers everything from radio to broadband, networks and 9-1-1, and facilities and operations. We provide confidence and support every step of the way, from design and procurement to building and management. The result is a high-performing public safety system that achieves maximum value and optimal efficiency. Additional information and career opportunities are available at www.MissionCriticalPartners.com.

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit www.BoozAllen.com.