

Federal Communications Commission



Task Force on Optimal Public Safety Answering Point Architecture (TFOPA)

*Working Group 2
Phase II Supplemental Report:
NG9-1-1 Readiness Scorecard*

December 2, 2016

Table of Contents

Contents

1	INTRODUCTION.....	4
2	TFOPA WORKING GROUP 2 MEMBERS	9
3	NG9-1-1 READINESS SCORECARD.....	11
3.1	BACKGROUND.....	11
3.1.1	Scope	11
3.1.2	Limitations	11
3.1.3	Purpose	11
3.2	NG9-1-1 DEFINITION.....	12
3.3	NG9-1-1 IMPLEMENTATION CONTINUUM.....	12
3.4	NG9-1-1 READINESS SCORECARD.....	14
3.4.1	Scorecard Explanation	14
3.4.2	NG9-1-1 Readiness Scorecard	17
3.5	NG9-1-1 SELF-ASSESSMENT MATRIX	22
3.5.1	Explanation	22
3.5.2	NG9-1-1 Self-Assessment Matrix	23
4	IMPORTANT CONSIDERATIONS.....	28
4.1	GOVERNANCE	28
4.1.1	Explanation	28
4.1.2	Governance Considerations Matrix	29
4.2	OSP ACCESS TO NG9-1-1 SYSTEMS	45
4.3	ESINET	46
4.4	SECURITY	47
4.4.1	Identification/Discovery	47
4.4.2	Assess/Prioritize	48
4.4.3	Implement/Operate	48
4.4.4	Monitor and Evaluate.....	51
4.4.5	Test/Evaluate.....	52
4.4.6	Improve/Evolve.....	52
4.5	SIZING.....	52
4.6	RESILIENCY, QUALITY AND SERVICE LEVELS	53
4.7	NETWORK MANAGEMENT	53
4.8	CROSS ENTITY INTERCONNECTIONS AND OPERATIONS	53
4.9	NG9-1-1 OPERATIONAL IMPACTS	53
4.9.2	Operational Aspects of NG9-1-1	55
4.9.3	Technical Considerations	57
4.9.4	Processing System Alarms	57
4.9.5	Data Management	58
4.9.6	NG9-1-1 Implementation Planning.....	59
4.10	STAFFING AND TRAINING	61
4.10.1	Introduction	61
4.10.2	Current Staffing Formulas, Profiles and Reports	63
4.10.3	NG9-1-1 Staffing and Special Considerations.....	64

4.11	LESSONS LEARNED: ESINET EARLY ADOPTER CASE STUDIES	65
4.11.1	<i>Introduction</i>	65
4.11.2	<i>Early Adopter Case Study Participants</i>	66
4.11.3	<i>Case Study Details</i>	67
4.11.4	<i>Conclusions</i>	70
5	RECOMMENDATIONS	72
6	CONCLUSIONS	74
7	APPENDICES	76
7.1	ESINET EARLY ADOPTER CASE STUDY INTERVIEW RESPONSES	76
7.2	RESOURCES	88
7.3	ACRONYMS	89
7.4	GLOSSARY OF TERMS	93

1 Introduction

The Task Force on Optimal PSAP Architecture (TFOPA)¹ is a federal advisory committee chartered under the Federal Advisory Committee Act (FACA)² to provide recommendations to the Federal Communications Commission (FCC) regarding actions Public Safety Answering Points (PSAPs) and 9-1-1 Authorities might take to enhance security, operations, and funding as Next Generation 9-1-1 (NG9-1-1) migration occurs.

The FCC directed TFOPA “to study and report findings and recommendations on structure and architecture in order to determine whether additional consolidation of PSAP infrastructure and architecture improvements would promote greater efficiency of operations, safety of life, and cost containment, while retaining needed integration with local first responder dispatch and support.”³ While the original direction of TFOPA was to consider PSAP “consolidation” as an option, Work Group 2 expanded the direction to include a number of other configuration alternatives available to 9-1-1 Authorities.

On 29 January 2016, TFOPA released an Adopted Final Report⁴, completing the work of Phase I. This report included detailed guidance resulting from efforts by three Task Force Working Groups.⁵ The report also listed a number of recommendations from these Working Groups for further discussion and consideration beyond the Final Report.

In Phase II of TFOPA, the Working Groups were charged with four tasks:⁶ 1) an In Depth Review of Emergency Communications Cybersecurity Center (EC3) Concept, 2) NG9-1-1 Readiness Scorecard, 3) Workforce Training and Education, and 4) Funding Sustainment Model.

Section 5 of the Phase I Report, titled “Optimal Approach to NG9-1-1 Architecture Implementation by PSAPs⁷,” was written by Working Group 2 (WG2). Section 5 delivered a Next Generation 9-1-1 environment foundation as well as a discussion of the NG9-1-1 “Ecosystem”. This term identifies the functional components necessary for the required transition to NG9-1-1.

WG2 discussion has led to broadening the scope of this activity, recognizing the critical/essential role of the PSAP while simultaneously acknowledging the 9-1-1 Authority and PSAP role in the end-state of a NG9-1-1 Ecosystem.

The following diagram,⁸ as presented in the TFOPA Phase I Final Report, illustrates the role of the PSAP in a fully deployed NG9-1-1 end state. In preparation for the content of this Supplemental Report, the reader should familiarize themselves with the relationships of the NG9-1-1 components and their purposes as depicted in Figure 3-1 and surrounding text in the Final Report.

¹ <https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point>

² <http://www.gsa.gov/portal/content/100916>.

³ <https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point>

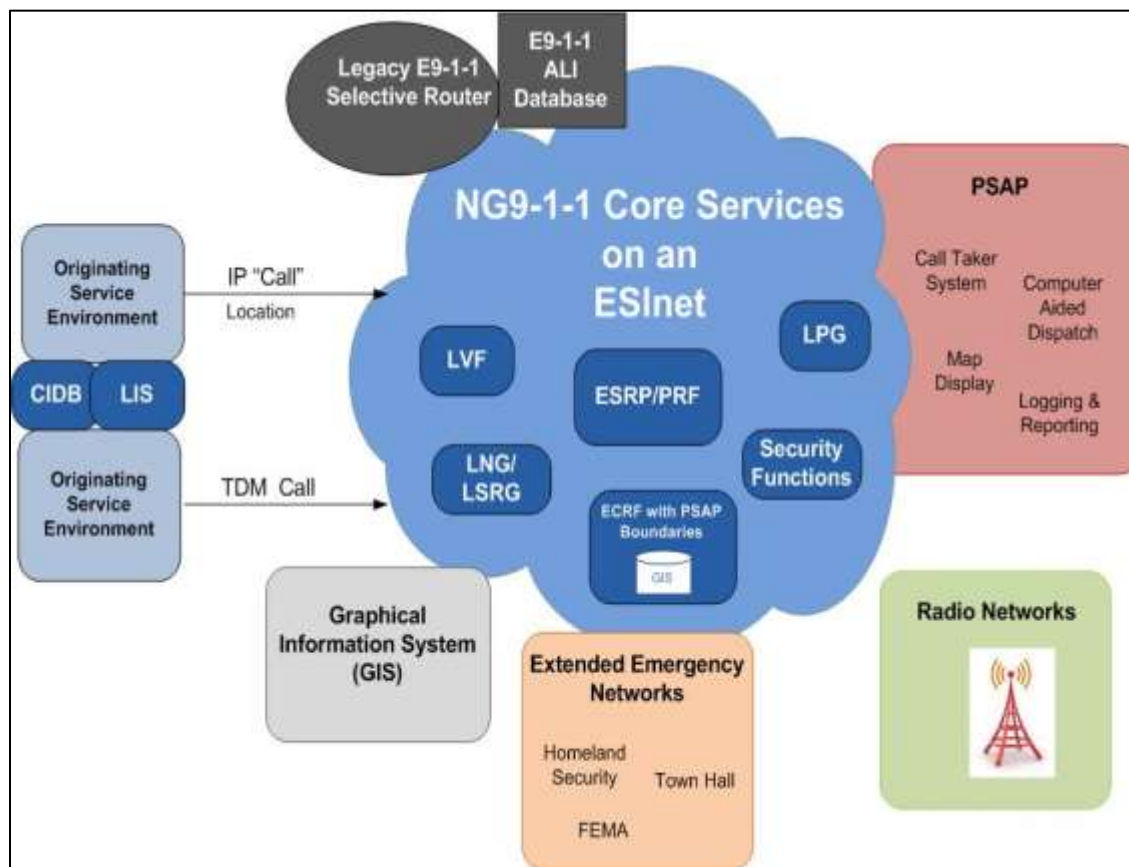
⁴ https://transition.fcc.gov/pshs/9-1-1/TFOPA/TFOPA_FINALReport_012916.pdf.

⁵ Working Group 1: Optimal Approach to Cybersecurity for PSAPs; Working Group 2: Optimal Approach to NG9-1-1 Architecture Implementation by PSAPs; and, Working Group 3: Optimal Approach to Next-Generation 9-1-1 Resource Allocation for PSAPs.

⁶ Tim May email dated 29 January 2016 405 PM.

⁷ <https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point> .

⁸ <https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point>



As plans for and implementation of NG9-1-1 systems continue, the 9-1-1 community has an opportunity to embrace the new NG9-1-1 Paradigm to enhance existing and build new cooperative relationships/partnerships. The 9-1-1 community will continue to make progress in transitioning the 9-1-1 system from legacy to full “end state” deployment of NG9-1-1 as described in this document.

In the Phase I Final Report,⁹ WG2 characterized NG9-1-1 transition as a three-step continuum - current Legacy, evolving through a “transitional” state, and, finally arriving at NG9-1-1. In WG2’s Phase II discussions, a more evolved conceptual model developed of the transitional steps to NG9-1-1. The new model adds “Foundational” following Legacy, then an “Intermediate” step after transitional with two end-states. The first end state is the 9-1-1 Authority’s “Jurisdictional End State” while the final-end state is that of the evolution to a “National End State”. Work Group 2’s revised transitional steps are depicted in the diagram below:

⁹ FCC, TFOPA, <https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point>.



Today, many 9-1-1 Systems and Agencies remain in the Legacy State. The transition to NG9-1-1 requires commitments from many groups including the 9-1-1 community, as well as industry. The slow transition has been impacted by many factors, including but not limited to:

- The absence of agency buy-in resulting from a lack of understanding of the elements associated with a transition to the NG9-1-1 end state
- Inadequate funding
- Incomplete or incoherent recognized standards
- Lack of stakeholder outreach
- Potential job losses
- Day-to-day demands which do not afford the time to plan for such a significant change.

This lingering development will result in crisis as the time-division multiplexing (TDM) switched Legacy 40 plus year old current platform of today is overwhelmed by the rapidly emerging internet protocol (IP) platform unless progress can be made to move to the NG9-1-1 end-state.

One ongoing task for WG2 was to further refine and define NG9-1-1 Ecosystem components. A second ongoing task for WG2 was to assist PSAPs, 9-1-1 Authorities, other government entities, policy development groups and all parties committed to NG9-1-1 in advancing more rapidly to “end state” deployments. This assistance includes the planning process, framework development, and implementation checklist (scorecard) development necessary to move from legacy, to transitional, to intermediate, to fully deployed end state NG9-1-1.

PSAPs should work with their redefined, as applicable, 9-1-1 Authorities to create an overall plan and progression chart for their situation.

In cases where there is no established 9-1-1 Authority, PSAPs may choose to first consider addressing their organizational approach to governance and financial capabilities to move forward. NG9-1-1 planning, whether at the regional or state level, should include the basic migration steps, or those locally modified, discussed in the TFOPA Final Report and this Supplemental Report to move toward the more detailed functional capabilities and functional elements.

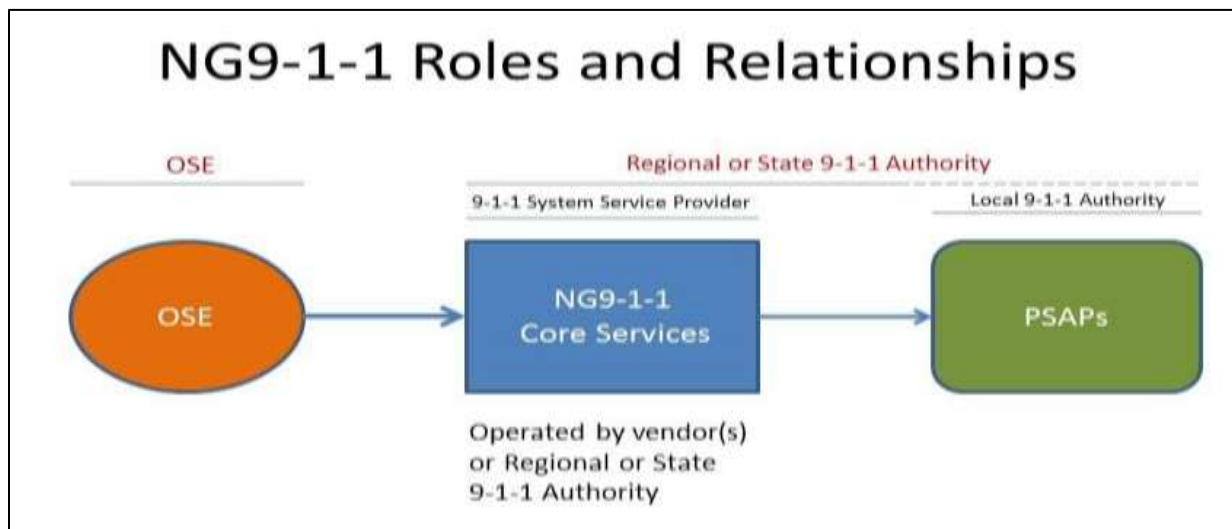
The below diagram illustrates the NG9-1-1 Roles and relationships for deployment of NG9-1-1 services. This relationship will also involve the Originating Service Environment (OSE) which is the NG9-1-1 expansion of the legacy Originating Service Provider (OSP). In many cases, this has been the telecom carriers.

WG2's continued goal is to further refine and define to component parts of the Ecosystem what is and will be Next Generation 9-1-1 to assist PSAPs, 9-1-1 Authorities, government interests, policy development groups and all parties committed to NG9-1-1 in the planning, framework, and implementation checklist (scorecard) necessary to move from legacy, to transitional, to intermediate, to fully deployed end state NG9-1-1.

PSAPs should work with their redefined 9-1-1 Authority to create an overall plan and progression chart for their situation.

In cases where there is no established 9-1-1 Authority, PSAPs should first address their organizational approach and financial capabilities to move forward. Any NG9-1-1 planning, whether at the regional or state level, should include the basic migration steps discussed in the TFOPA Final Report and this Supplemental Report to move toward the more detailed functional capabilities and functional elements.

The below diagram further illustrates the NG9-1-1 Roles and relationships that need to be developed in evolving to any end state deployment of NG9-1-1 services. This relationship will also involve the Originating Service Environment (OSE) which is the NG9-1-1 expansion of the legacy Originating Service Provider (OSP); e.g.-carriers.



TFOPA WG2 Phase II work continued from where the January 2016 Final Report concluded. WG2 expanded the framework for NG9-1-1 planning, delivered a detailed NG9-1-1 Scorecard (to identify the transition requirements a 9-1-1 Authority will need to meet moving forward), discussed the training and education that will be necessary, and studied the lessons learned in the implementation of data transport foundations through ESInets.

TFOPA WG2 hopes that PSAP managers, 9-1-1 Authority managers, elected officials at the local, state, tribal and federal levels come to an understanding to create NG9-1-1 end states regionally, at the state level and the national level. All efforts should be made to compress the timeline of this development and implementation so as to manage it in a planned evolution as opposed to a crisis managed reactionary implementation as TDM is replaced by IP technology.

2 TFOPA Working Group 2 Members

Name	Organization Represented	Title	Participation
Michael Connelly	FCC	FCC Liaison	
Working Group 2 Leadership			
Steve Souder	Fairfax County VA	Director of 9-1-1 / Public Safety Comm.	TFOPA Chairman
Dana Wahlberg	State of Minnesota	9-1-1 Program Manager	TFOPA Vice Chair
David Holl	Lower Allen Twp., PA	Director of Public Safety	WG2 Chairman
Roger Hixson	NENA	Technical Issues Director	WG2A Co-Chair
Bill Mertka	Motorola	Sr. Product Planning Consultant	WG2A Co-Chair
Jeff Wittek	Airbus DS Communications	Chief Strategic Officer	WG2B Co-Chair
Mary Boyd	West Safety Services	VP External Affairs	WG2B Co-Chair WG2C Co-Chair
April Heinze	INdigital	Industry Affairs Specialist	WG2C Co-Chair
Alicia Burns	The Digital Decision	NG9-1-1 Consultant	WG2D Co-Chair
Working Group 2 Members			
Bernard Aboba	Microsoft - Skype	Principal Architect	WG2A
Bradley Blanken	Competitive Carrier Association	VP – Industry Development	WG2C
Ron Bloom	Frontier Communications	9-1-1 Services Manager	WG2D
Alfredo Bocanegra	9-1-1ResQ	CEO	WG2B, WG2C
Daryl Branson	Colorado Public Utilities Commission	Sr. 9-1-1 Telecom Analyst	WG2D
Bob Brown	NPSTC	IT Manager, NH 9-1-1	WG2A, WG2B
Laurie Flaherty	NHTSA	Coordinator, National 9-1-1 Program Office	WG2B
Mark Fletcher	Avaya	Chief Architect	WG2A, WG2B, WG2C

Name	Organization Represented	Title	Participation
Jim Goerke	Texas 9-1-1 Alliance	CEO	WG2A, WG2B
Joe Heaps	NIJ / DOJ	Program Manager	WG2B, WG2D
Mike Nelson	West Safety Services	VP – Sr. Technical Officer	WG2A, WG2B
Dusty Rhoads	DHS/OEC	Branch Chief	WG2A, WG2B
Chuck Spalding	Palm Beach County, FL	Director NG9-1-1 Technical Services	WG2D
Chuck Vick	Verizon	E9-1-1 Group Manager	WG2A
Patti West	BRETSA, CO	Sr. Consultant for AltaVista Group	WG2C
Christy Williams	North Central Texas Council of Governments	Director of 9-1-1	WG2D

3 NG9-1-1 Readiness Scorecard

3.1 *Background*

3.1.1 Scope

As previously mentioned in this document, TFOPA is a federal advisory committee chartered by the FCC and represents subject matter expertise throughout the 9-1-1 industry. TFOPA is tasked with making recommendations to PSAP stakeholders regarding possible actions to optimize their security, operations and funding as PSAPs migrate to NG9-1-1. Work Group 2, as part of this report, delivers a tool for public safety entities to assess their level of NG9-1-1 readiness. The NG9-1-1 transition involves several maturity stages, from legacy 9-1-1 through the i3 End State¹⁰ in a fully featured NG9-1-1 ecosystem. Recognizing the importance of cybersecurity, Work Group 2 includes in the scorecard a set of identity, credentialing, and access management (ICAM) measures that may be used as a minimum set necessary to be in place for a 9-1-1 Authority to be NG9-1-1 ready.

3.1.2 Limitations

There is no end-to-end accredited technical standard for NG9-1-1. A lack of relevant, enforceable standards in the public safety communications ecosystem could decrease the likelihood of successful implementation of NG9-1-1. The NENA i3 architecture standard and other NENA NG9-1-1 standards are examples of applicable standards. The National 9-1-1 Program Office has created a compendium of standards.¹¹ Other standards are in development (e.g., ATIS/ESIF IMS, NENA, and APCO) and should be considered once promulgated.

The NG9-1-1 Readiness Scorecard does not constitute a standard as it has not been promulgated by a standards body. WG2 looks forward to the further development of collaborative, consensus-based NG9-1-1 standards promulgated by recognized standards bodies.

3.1.3 Purpose

The NG9-1-1 Readiness Scorecard identifies essential elements which are necessary to be present within each NG9-1-1 Implementation Maturity State as defined later in the document. It should be noted that the NG9-1-1 Readiness Scorecard is limited to essential elements and is not meant to be all inclusive.

The NG9-1-1 Readiness Scorecard provides a 9-1-1 Authority Stakeholder with a more granular understanding of essential NG9-1-1 system elements and enables a 9-1-1 Authority Stakeholder to assess their position within the NG9-1-1 Implementation Maturity Continuum. This understanding will allow a 9-1-1 Authority Stakeholder to better plan transition steps to move from legacy 9-1-1 through being in a fully functional NG9-1-1 end state. Additionally, by understanding essential NG9-1-1 system elements in each maturity state, a 9-1-1 Authority Stakeholder will be able to plan for and budget transition costs.

¹⁰ NENA, https://www.nena.org/default.asp?page=i3_Stage3.

¹¹ National 911 Program, https://www.911.gov/pdf/NG911-Standards-Identification-Analysis_03222016.pdf.

3.2 NG9-1-1 Definition

While there are multiple definitions of NG9-1-1, WG2 utilized the definition found in NENA's, "What is NG9-1-1".¹² NENA defined NG9-1-1 as "a system comprised of hardware, software, data and operational policies and procedures briefly described below, to:

- Provide standardized interfaces from call and message services
- Process all types of emergency calls including non-voice (multi-media) messages
- Acquire and integrate additional data useful to call routing and handling
- Deliver the calls/messages and data to the appropriate PSAPs and other appropriate emergency entities
- Support data and communications needs for coordinated incident response and management
- Provide a secure environment for emergency communications"

The NG9-1-1 Readiness Scorecard builds upon this definition by identifying essential hardware, software, data, operational policies/procedures, security and governance elements which are necessary to be present in each implementation maturity state (described in section 3). The PSAP and its operations (including dispatch) play an integral role in the delivery of NG9-1-1 services.

3.3 NG9-1-1 Implementation Continuum

NG9-1-1 can be implemented in a variety of ways (e.g., phased, single step implementation). Based on anecdotal information a "phased" implementation model offers the greatest opportunity for success. The NG9-1-1 Implementation Maturity Model, previously documented by the National 9-1-1 Program Office within the U.S. Department of Transportation in its DRAFT NG9-1-1 Functional and Technical Requirements document, is a well-crafted model and has been incorporated into the NG9-1-1 Readiness Scorecard with only minor modification. WG2 members began this work with varied levels of knowledge with regard to the Program Office's NG9-1-1 Implementation Maturity Model.¹³ The team/leadership believed our work should begin with a blank sheet of paper, independent of the Program Office's NG9-1-1 Implementation Maturity Model. Upon completion of this work, the WG2 members found overlap/consistency with much of the Program Office's NG9-1-1 Implementation Maturity Model, with minor modifications/adjustments, for example, addition of...a stage. In effect, while the group's work began with a blank piece of paper, a reader familiar with the Program Office's NG9-1-1 Implementation Maturity Model might believe this work built upon the Program Office's NG9-1-1 Implementation Maturity Model. The group understands this view.

The NG9-1-1 Implementation Continuum, employed within the WG2 NG9-1-1 Readiness Scorecard, utilizes the following NG9-1-1 Implementation Maturity States, which are substantially aligned with those in the aforementioned Program Office document;

¹² NENA, https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/ng9-1-1_project/whatisng9-1-1.pdf

¹³ National 911 Program, <http://www.911.gov/911Connects/NG911-cost-study-first-year-progress.html>.

- Legacy State

The Legacy stage is characterized as the point in time where 9-1-1 services are provided by the traditional incumbent local exchange carrier (ILEC) with circuit-switched infrastructure and Automatic Location Identification (ALI) circuits.

- Foundational State

As the name implies, the Foundational stage is where the groundwork and planning for NG9-1-1 implementation is initiated. NG9-1-1 feasibility studies are performed, Geographic Information System (GIS) data preparation commences, and IP networks may be implemented. NG9-1-1 systems are not yet operational and system procurement is either planned or underway

- Transitional State

The Transitional state is the point at which services have migrated partially from the legacy environment and the 9-1-1 services are enabled by an IP infrastructure. The Emergency Services IP Network (ESInet) is in place and ESN routing is still being utilized. This is the first state in which certain Next Generation Core Service elements may be implemented. At this point, a governance model has been established. Systems in this State are said to be NG9-1-1 Transitional.

- Intermediate State

The Intermediate State is the state in which the 9-1-1 Authority has implemented and made operational all i3 Core functions within their control and all calls are routed per GIS boundaries and location information (i3 algorithms). Additionally, an i3 PSAP multimedia call handling system (terminating ESRP) is implemented. Infrastructure and applications are being refined to incorporate advanced call- and data-delivery interfaces. Business and performance elements are maturing and are reviewed in regular intervals to optimize operations. Governance agreements are in place and the model is functioning. Systems in the Intermediate State are said to be NG9-1-1 READY.

- Jurisdictional End State¹⁴

The Jurisdictional End State is the state in which PSAPs are served by i3 standards-based systems and/or elements, from ingress through multimedia "call" handling. Originating Service Providers are providing SIP interfaces and location information during call set-up time. Within the jurisdiction, ESInets are interconnected providing interoperability which is supported by established agreements, policies and procedures. Systems in the End State are NG9-1-1 Compliant.

- National End State

The National End State is the state in which PSAPs are served by i3 standards-based systems and/or elements, from ingress through multimedia "call" handling. Nationally, ESInets are

¹⁴ Jurisdiction could be a Local, Regional, State or Tribal Authority and could be intrastate or interstate.

interconnected providing interoperability which is supported by established agreements, policies and procedures. All systems in the End State are NG9-1-1 Compliant.

3.4 NG9-1-1 Readiness Scorecard

3.4.1 Scorecard Explanation

The NG9-1-1 Readiness Scorecard provides 9-1-1 Authority stakeholders an understanding of essential elements within in each NG9-1-1 Implementation Maturity State. With this understanding 9-1-1 Authority stakeholders can better plan for the technical, operational and costs associated with their NG9-1-1 transition.

The NG9-1-1 Readiness Scorecard is broken down into the following areas of interest:

- Governance
- Routing & Location
- GIS Data
- NG Core Service Elements
- Network
- PSAP Call Handling System and Applications
- Security
- Operations
- Optional Interfaces

Each “area of interest” is broken down by a set of essential elements. The scorecard elements identify either functional capabilities, architecture implementation or operational capabilities. Functional and operational capabilities are either defined by legacy 9-1-1 capabilities or those capabilities defined by the NENA i3 standard. Architecture implementation is defined by either legacy compatibility or alignment to the NENA i3 standard. Section 4 provides important additional detail on the “areas of interest” under General Considerations, and as it relates to Operational Impacts of NG9-1-1.

3.4.1.1 Governance

Governance addresses the structured oversight¹⁵ of the 9-1-1 Authorities and identifies whether there is a governing body with documented and tracked planning and implementation efforts. Coordination indicates whether all participating entities within the jurisdictional scope have agreed upon cooperation and going forward strategies and plans. Funding and Resources indicate that the funding and resources necessary to execute the NG9-1-1 plan have been identified or a strategy is in place to secure those funds and resources as necessary points during the plan execution. Governance structure is ongoing, providing the coordination and administration of the entire NG9-1-1 service system after implementation.

3.4.1.2 Routing & Location

Routing and location defines the systematic approach that is used to determine 9-1-1 call routing and the supporting data functions. Legacy 9-1-1 calls are processed by relating the calling telephone number to an Emergency Services Number (ESN) that then defines the primary and secondary PSAPs. NG9-1-1 utilizes geospatial routing by using the caller’s location information and a set of PSAP jurisdictional polygons to determine the primary PSAP. A “pure” NG9-1-1 implementation assumes OSPs have changed the means by which they deliver 9-1-1 calls, but it is not realistic or expected that OSPs will

¹⁵ As defined by legislative, regulatory, executive order, 9-1-1 Authority or other relevant agreements.

change together or even all complete their changes any time soon. Therefore, the model is complicated by mechanisms to “transition” from legacy methods to NG9-1-1 methods. The legacy ALI DBMS provides location information based on the caller’s telephone number and it or its equivalent is required until all OSPs deliver location information with their 9-1-1 call setup messages or provide LIS capabilities. The National Forest Guide is a capability necessary when Nationwide OSPs require a capability to determine to which ESInet to direct a given 9-1-1 call. “Hierarchical Forest Guides Populated” indicates a provisioning capability for various Forest Guides to share the routing polygon (ESInet or PSAP Jurisdictional boundary) information.

3.4.1.3 GIS Data

GIS Data is a fundamental element of NG9-1-1 but is not utilized for legacy 9-1-1 call routing. These selection items define steps to plan, process and utilize GIS data for NG9-1-1. Selection items are included that represent the NENA i3 functional elements that receive and utilize GIS data to complete call routing functions. The exchange of jurisdictional boundaries indicates an automated mechanisms where an ESInet ECRF (or Forest Guide function) automatically keeps a neighboring ESInet ECRF (or Forest Guide function) updated with its jurisdictional polygons to allow for 9-1-1 call hand-offs and call transfers. GIS data is also utilized with NG9-1-1 for the validation (LVF) function and to support mapping services for the PSAPs.

3.4.1.4 NG9-1-1 Core Service Elements

The central Core Services functions provide the logical processing interactions between the delivery of calls and data from the OSE, additional data, and delivery to PSAPs, and provide the features to support management of how the NG9-1-1 service accomplishes this under normal and abnormal conditions. NG Core Service Element capabilities are an itemized list of the functional capabilities defined by the NENA i3 architecture. As stated in the NENA i3 specification, it is not appropriate to identify a box or component that performs the functional services, but instead just to identify that the infrastructure somehow does accomplish the functional capabilities defined for each item. Except for the “Border Control Function (BCF)”, this area of interest is not applicable to IP Selective Router (IPSR) scenarios. These selection items become relevant when the NG9-1-1 transitional architecture is implemented through the time period that the NG9-1-1 end-state is achieved, e.g., when all OSPs deliver 9-1-1 services via IP protocols and include delivery of location information at call setup time. NG Core Service operations, organizational planning and staffing are discussed in the relevant Important Considerations section below.

3.4.1.5 Network (OSE and ESInet)

The network area capabilities represent the various technology mechanisms for connecting external entities to either a legacy selective router or functions within an ESInet for the purposes of processing 9-1-1 calls. Legacy call circuit mechanisms are primarily TDM based technology (e.g., SS7, CAMA) and NG9-1-1 moves to IP based technology with application specific protocols such as SIP and RTP. In some cases, IP technology can be deployed as a replacement for a legacy TDM technology before completely embracing the NENA i3 defined functional interface model, such as, an OSP using IP technology call delivery to an ESInet IP Selective Router without including a location object representing the caller’s location. E2 Circuits are the legacy Wireless capabilities to retrieve location information and will be required until all OSPs that allow location update transactions deliver caller’s location information at call setup time. ESInet to ESInet connections will occur as neighboring jurisdictions implement ESInets and require the ability to exchange 9-1-1 calls.

3.4.1.6 PSAP Call Handling System and Applications

Legacy Call Handling Systems are defined by their use of CAMA trunk interfaces and legacy ALI interfaces. The first step toward NG9-1-1 is upgrading call handling equipment to be IP technology based system and optionally may include replacing the legacy CAMA TDM circuits with the ATIS defined IP technology based transitional RFAI protocol. The NENA i3 defined functional entities interact with PSAP CHS and other applications via the IP based interface protocols referenced within the NENA i3 specification. An i3 PSAP would implement all the NENA i3 defined protocols (including SIP, RTP, HTTPs, LoST and HELD) and the i3 compliant software to allow interaction with NG Core Service functions. An i3 PSAP Multimedia Call Handling System,¹⁶ which includes a terminating ESRP, is required to be present in an NG9-1-1 end state system.

Mapping is the capability to display caller's location information on a map at the PSAP's 9-1-1 Call Handling positions. Interim Text-to-9-1-1 (SMS) is the capability of an OSP provided Text Control Center (TCC) to message to a PSAP, but, ultimately the TCC can interface to the NENA i3 functional elements that then deliver Text-to-9-1-1 to the PSAP CPE while incorporating NG9-1-1 policy rules. Multimedia refers to both Real Time Text (RTT) capabilities and services such as a PSAPs ability to receive video from external sources as a data application. Logging & Recording at the PSAP is per local PSAP functions.

3.4.1.7 Security

Security includes capabilities, operations and best practices expected at the ESInet, the NENA i3 functional elements, PSAP and all external facing interfaces.

3.4.1.8 Operational Planning

Operations planning addresses aspects of execution, oversight, plan management and efforts to support on-going evolution with the planning of NG Core Services, ESInet and PSAP operations and the transition to the NG9-1-1 processing model and services.

3.4.1.9 Optional Interfaces

Optional Interfaces addresses services and interfaces that interconnect with the ESInet but apply beyond NG Core Services primary functions, although these functions may otherwise appear necessary and prudent. Any and all optional interfaces must comply with all applicable industry interface standards and shall not interfere with or impact the function or security of the NG9-1-1 systems.

¹⁶ See Section 3-Operational or Technical Description, NENA/APCO-REQ-001.1.1-2016, NENA/APCO Next Generation 9-1-1 Public Safety Answering Point Requirements, https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA-APCO-REQ-001.1.1-2016_N.pdf

3.4.2 NG9-1-1 Readiness Scorecard

Next Generation 9-1-1 Readiness Scorecard						
<u>Category</u>	NG9-1-1 Implementation Maturity State					
	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State - Jurisdictional</u>	<u>i3 End State - National</u>
<u>Governance</u>						
Governance Structure Design & Framework	Optional	X	X	X	X	X
Strategic Planning	Optional	Optional	X	X	X	X
Coordination	Optional	Optional	X	X	X	X
Funding & Resources	Optional	X	X	X	X	X
<u>Routing & Location</u>						
Selective (ESN) Routing	X	X				
IP Selective (ESN) Routing			X			
Geospatial Routing (utilizing best available location)				X	X	X
ALI DBMS	X	X	X	X		
LIS				Optional	X	X
National Forest Guide contains Jurisdictional ESInet Authoritative Boundary					Optional	X
If applicable, Hierarchical Forest Guides Populated					Optional	X

Next Generation 9-1-1 Readiness Scorecard						
<u>Category</u>	NG9-1-1 Implementation Maturity State					
	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State - Jurisdictional</u>	<u>i3 End State - National</u>
<u>GIS Data</u>						
NG9-1-1 Dataset Creation Project Planned		X				
NG9-1-1 Dataset Creation Project in-Progress		X	Optional			
NG9-1-1 Dataset Complete				X	X	X
Data formatted for Location Verification Function (LVF)			Optional	Optional	X	X
Data formatted for Emergency Call Routing Function (ECRF)			Optional	X	X	X
Data formatted for Policy Routing Function (PRF)			Optional	X	X	X
Jurisdictional Boundaries exported to neighboring ESInets					Optional	X
<u>NG Core Service Elements</u>						
Legacy Selective Router Gateway (LSRG)			Optional	X	Optional	Optional
Location Verification Function (LVF)			Optional	Optional	X	X
Emergency Services Routing Proxy (ESRP)			Optional	X	X	X
Emergency Call Routing Function (ECRF)			Optional	X	X	X

Next Generation 9-1-1 Readiness Scorecard						
<u>Category</u>	NG9-1-1 Implementation Maturity State					
	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State - Jurisdictional</u>	<u>i3 End State - National</u>
Legacy Network Gateway (LNG)			Optional	X	Optional	Optional
Legacy PSAP Gateway (LPG)			Optional	X	Optional	Optional
Border Control Function (BCF)			Optional	X	X	X
Logging				X	X	X
<u>Network</u>						
OSP / OSE			X	X	X	X
Ingress Network - Non-IP	X	X	X	X		
Egress Network - Non-IP	X	X				
Traditional ALI Data Circuits	X	X	X			
Ingress - IP (ESInet)			Optional	X	X	X
Egress - IP (ESInet)			X	X	X	X
Interconnects beyond ESInet boundary *				X	X	X
E2 Circuits	X	X	X	X		
Neighboring ESInet Interconnection for Call Hand-offs and Transfers				Optional	Optional	X

Next Generation 9-1-1 Readiness Scorecard						
<u>Category</u>	NG9-1-1 Implementation Maturity State					
	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State - Jurisdictional</u>	<u>i3 End State - National</u>
<u>PSAP Call Handling System & Applications</u>						
Legacy Call Handling System	X	X				
IP based Call Handling System			X			
i3 PSAP (Terminating ESRP) Multimedia Call Handling System			Optional	X	X	X
Mapping			X	X	X	X
Text-to-9-1-1 (SMS)			X	X	X	X
Multimedia				X	X	X
Logging & Recording				X	X	X
<u>Security</u>						
Identification/Discovery		X	X	X	X	X
Assess/Prioritize		X	X	X	X	X
Implement/Operate			X	X	X	X
Monitor/Analyze			Optional	X	X	X

Next Generation 9-1-1 Readiness Scorecard						
<u>Category</u>	NG9-1-1 Implementation Maturity State					
	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State - Jurisdictional</u>	<u>i3 End State - National</u>
Operations						
NG9-1-1 Operational Planning in Progress		X				
Amount of Staff Needed		X				
NG9-1-1 Operational Procedures Developed			Optional	X	X	X
NG9-1-1 Operation Procedures Implemented			Optional	X	X	X
Training Staff		Optional	X	X	X	X
9-1-1 Plan Update		X				
<u>Optional Interfaces</u>						
CAD			Optional	Optional	Optional	Optional
Broadband Field Network			Optional	Optional	Optional	Optional
Additional Data				Optional	Optional	Optional
Personal Information Data				Optional	Optional	Optional

3.5 NG9-1-1 Self-Assessment Matrix

3.5.1 Explanation

Used in conjunction with the NG9-1-1 Readiness Scorecard, the NG9-1-1 Self-Assessment Matrix enables a 9-1-1 Authority Stakeholder (or designee) to determine its current status within the NG9-1-1 implementation continuum and assist a 9-1-1 Authority in identifying the steps necessary to reach the next NG9-1-1 implementation maturity state. A 9-1-1 Authority completes the Self-Assessment Matrix by filling in the current implementation status of specific functions, components, policies and processes and comparing their status against the NG9-1-1 Readiness Scorecard Maturity Continuum to identify in which NG9-1-1 implementation state they fit.

3.5.2 NG9-1-1 Self-Assessment Matrix

Next Generation 9-1-1 Self-Assessment			
	NG9-1-1 Maturity State Self-Assessment		
<u>Category</u>	<u>Status</u>	<u>Maintained/Provided by</u>	<u>Notes</u>
<u>Governance</u>			
Governance Structure Design & Framework			
Strategic Planning			
Coordination			
Funding & Resources			
<u>Routing & Location</u>			
Selective (ESN) Routing			
IP Selective (ESN) Routing			
Geospatial Routing (utilizing best available location)			
ALI DBMS			
LIS			
National Forest Guide contains Jurisdictional ESInet Authoritative Boundary			
If applicable, Hierarchical Forest Guides Populated			

Next Generation 9-1-1 Self-Assessment			
	NG9-1-1 Maturity State Self-Assessment		
<u>Category</u>	<u>Status</u>	<u>Maintained/Provided by</u>	<u>Notes</u>
<u>GIS Data</u>			
NG9-1-1 Dataset Creation Project Planned			
NG9-1-1 Dataset Creation Project in-Progress			
NG9-1-1 Dataset Complete			
Data formatted for Location Verification Function (LVF)			
Data formatted for Emergency Call Routing Function (ECRF)			
Data formatted for Policy Routing Function (PRF)			
Jurisdictional Boundaries exported to neighboring ESInets			
<u>NG Core Service Elements</u>			
Legacy Selective Router Gateway (LSRG)			-
Location Verification Function (LVF)			
Emergency Services Routing Proxy (ESRP)			
Emergency Call Routing Function (ECRF)			
Legacy Network Gateway (LNG)			
Legacy PSAP Gateway (LPG)			

Next Generation 9-1-1 Self-Assessment			
	NG9-1-1 Maturity State Self-Assessment		
<u>Category</u>	<u>Status</u>	<u>Maintained/Provided by</u>	<u>Notes</u>
Border Control Function (BCF)			
Logging			
<u>Network</u>			
OSP / OSE			-
Ingress Network - Non-IP			
Egress Network - Non-IP			
Traditional ALI Data Circuits			
Ingress - IP (ESInet)			
Egress - IP (ESInet)			
Interconnects beyond ESInet boundary *			
E2 Circuits			
Neighboring ESInet Interconnection for Call Hand-offs and Transfers			
<u>PSAP Call Handling System & Applications</u>			
Legacy Call Handling System			

Next Generation 9-1-1 Self-Assessment			
	NG9-1-1 Maturity State Self-Assessment		
<u>Category</u>	<u>Status</u>	<u>Maintained/Provided by</u>	<u>Notes</u>
IP based Call Handling System			
i3 PSAP (Terminating ESRP) Multimedia Call Handling System			
Mapping			
Text-to-9-1-1 (SMS)			
Multimedia			
Logging & Recording			
<u>Security</u>			
Identification/Discovery			
Assess/Prioritize			
Implement/Operate			
Monitor/Analyze			
<u>Operations</u>			
NG9-1-1 Operational Planning in Progress			
Amount of Staff Needed			
NG9-1-1 Operational Procedures Developed			

Next Generation 9-1-1 Self-Assessment			
	NG9-1-1 Maturity State Self-Assessment		
<u>Category</u>	<u>Status</u>	<u>Maintained/Provided by</u>	<u>Notes</u>
NG9-1-1 Operation Procedures Implemented			
Training Staff			
9-1-1 Plan Update			
<u>Optional Interfaces</u>			
CAD			
Broadband Field Network			
Additional Data			
Personal Information Data			

4 Important Considerations

4.1 Governance

4.1.1 Explanation

The following Governance considerations matrix is designed to assist authorities in developing a formalized NG9-1-1 Strategic Plan by identifying specific requirements or components. Implementation of a Strategic Plan ensures formalized Governance Models are in place to aid in the transition between Legacy 9-1-1 system, Interim Maturity States, and ultimately achieve the End State Goal of a fully functional i3 NG9-1-1 System. The Governance matrix details critical milestones that should be included in the NG9-1-1 planning considerations and the guide includes critical elements such as:

- Development of a formalized 9-1-1 Planning Authority;
- 9-1-1 Coordinator Designation;
- Regional Planning;
- Formalized Participation Agreements if not legislative mandated;
- Formalized Memorandum of Understanding Among Stakeholders;
- Intra and Inter-State Planning Considerations;
- PSAP Operational Impact Planning;
- Information Sharing and Collaboration;
- Outreach Programs;
- Funding & Funds Management

4.1.2 Governance Considerations Matrix

Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
<u>Item</u>	<u>Governance</u>						
1	Governance Structure (State)						
1a	Develop a Name, Authority, and Purpose for a formalized state 9-1-1 governance body that solidifies the legal standing of the governing body and the purpose of its establishment. Indicate where the authority derives from (i.e. state or federal statutes) and if it amends or supersedes any prior authority.		Optional	Required	Required	Required	Required
1b	Define in detail what the state governance body has the authority to oversee, including any rule-making authority, aligning activities to overarching strategies and plans (i.e., State 9-1-1 plan, SCIP, NECP) and maintaining fiduciary and fiscal compliance.		Optional	Required	Required	Required	Required
1c	Develop a charter or bylaw that builds upon the legal authority (e.g., Executive Order or statute) or sets the agreed upon authority (e.g., ad-hoc groups)		Optional	Required	Required	Required	Required
1d	Provide a reporting mechanism for the state governance body to notify the public, Executive and Legislative Branch on accomplishments, issues, and future priorities to enhance 9-1-1/NG9-1-1.		Optional	Required	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
1e	Populate membership of state 9-1-1 governance authority. Invite state and local representatives (i.e., SWIC, relevant statewide broadband authority e.g., SPOC, statewide broadband authority, and 9-1-1 Administrator).	1a	Optional	Required	Required	Required	Required
1f	Indicate roles, responsibilities and functions (e.g., voting, non-voting, and <i>ex-officio</i>) for members of the state authority	1a	Optional	Required	Required	Required	Required
1g	Establish a 9-1-1 Administrator (and appropriate support) to facilitate the statewide implementation of 9-1-1 services, including but not limited to operations, training, identification and recommendation of minimum performance standards, for systems and personnel.		Optional	Required	Required	Required	Required
1h	Establish ongoing mechanism to facilitate 9-1-1/Public Safety Broadband collaboration (e.g., SWIC, statewide broadband authority, and State 9-1-1 Administrators are members of the state governance structure).		Optional	Optional	Required	Required	Required
2	Governance Structure (Regional)						

Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
2a	Develop a Name, Authority, and Purpose for a formalized regional governance structure that solidifies the legal standing of the governing body and the purpose of its establishment. Indicate where the authority derives from (e.g., statute/regulation) and if it amends or supersedes any prior authority. If interstate applies, confirm concurrence of state governments.		Optional	Required	Required	Required	Required
2b	Define in detail what the regional governance body has the authority to oversee, including any rule-making authority, aligning activities to overarching strategies and plans (e.g., state/regional 9-1-1 plan), and maintaining fiduciary and fiscal compliance. If interstate applies, confirm concurrence of state governments.		Optional	Required	Required	Required	Required
2c	Develop a charter or bylaw that builds upon the legal authority (e.g., Executive Order or statute) or sets the agreed upon authority (e.g., ad-hoc groups). If interstate applies, confirm concurrence of state governments.		Optional	Required	Required	Required	Required
2d	Provide a reporting mechanism for the regional governance body to notify the public and all appropriate state and regional government agencies and bodies on accomplishments, issues, and future priorities to enhance 9-1-1/NG9-1-1.		Optional	Required	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>			NG9-1-1 Implementation Maturity State				
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
2e	Identify a mutually agreed upon entity with the ability to provide administrative support or develop a mechanism to share these responsibilities.		Optional	Optional	Optional	Optional	Optional
2f	Populate membership of regional 9-1-1 governance authority.	1a	Optional	Required	Required	Required	Required
2g	Indicate roles, responsibilities and functions (e.g., voting, non-voting, and ex-officio) for members of the regional authority		Optional	Required	Required	Required	Required
2h	If interstate applies, establish equitable/acceptable representation and authority among member states.		Optional	Required	Required	Required	Required
2i	If interstate applies, invite the SWIC, FirstNet statewide broadband authority/relevant FirstNet state point of contact, and 9-1-1 Administrator(s) to become members, advisors, chairs, or some combination.		Optional	Required	Required	Required	Required
2j	If intrastate applies, encourage participation by senior officials of relevant entities.		Optional	Optional	Optional	Optional	Required
2k	If intrastate applies, invite state representatives (e.g. SWIC, FirstNet statewide broadband authority/relevant FirstNet state point of contact, and 9-1-1 Administrator).		Optional	Optional	Optional	Optional	Optional
2l	Ensure all emergency communications capabilities are invited to participate on the governance structure (LMR, broadband, 9-1-1, alerts and warnings functions, etc.), at all levels of government.		Optional	Optional	Optional	Optional	Optional

Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
3	Governance Structure (Local)						
3a	Develop a Name, Authority, and Purpose for the formalized local 9-1-1 governance structure that solidifies the legal standing of the governing body and the purpose of its establishment. Indicate where the local authority derives from and if it amends or supersedes any prior authority,		Required	Required	Required	Required	Required
3b	Define in detail, local governance body oversight authority, including, but not limited to, rulemaking, aligning activities to state/national strategies and plans (i.e., State 9-1-1 Plan, SCIP, NECP) and maintaining fiduciary and fiscal compliance.		Required	Required	Required	Required	Required
3c	Develop a charter or bylaw that builds upon the legal authority (e.g., statute) or sets the agreed upon authority (e.g., ad-hoc groups)		Required	Required	Required	Required	Required
3d	Provide a reporting mechanism for the local governance body to formally notify the public, and all appropriate state and local government agencies and bodies on accomplishments, issues, and future priorities to enhance 9-1-1/NG9-1-1.		Optional	Required	Required	Required	Required
3e	Populate membership of local 9-1-1 governance authority.	3a	Optional	Required	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
3f	Indicate roles, responsibilities and functions (e.g., voting, non-voting, and ex-officio) for members of the local authority		Optional	Required	Required	Required	Required
3g	Establish a 9-1-1 Administrator (and appropriate support) to facilitate the local implementation of 9-1-1 services, including but not limited to operations, training, identification and recommendation of minimum performance standards, for systems and personnel.		Optional	Required	Required	Required	Required
3h	Establish ongoing mechanism to facilitate 9-1-1/Public Safety Broadband collaboration and encourage membership of 9-1-1 and Broadband representatives on each other's local governance structures. Potential collaborators may include Chief or Department Head-level members from fire, law enforcement and public service leaders. Attempt to include members from law enforcement, fire and emergency services, emergency medical services, emergency management, public safety communications, public safety coordination and fusion centers, public works, and non-governmental entities.		Optional	Optional	Required	Required	Required
4	Governance Planning (State)						
4a	Based on authority, establish requirements for compliance with standards and policy for state-funded PSAP operations.		Optional	Required	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>			NG9-1-1 Implementation Maturity State				
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
4b	Develop and adopt a 9-1-1/NG9-1-1 state plan		Optional	Optional	Required	Required	Required
4c	Establish authority for a state entity to collaboratively plan the entire or certain components of the NG9-1-1 network (for example: deploy Emergency Service IP Network (ESInet))		Optional	Required	Required	Required	Required
4d	State governance body aligns the SCIP, general 9-1-1 initiatives and the state NG9-1-1 strategic plan. Updated SCIPs to reflect 9-1-1 emergency communications goals and objectives		Optional	Optional	Optional	Required	Required
4e	Develop and submit reports on 9-1-1/NG9-1-1 progress to applicable authorities (e.g. the National 9-1-1 Office annual 9-1-1 census), including all reports submitted by local and regional agencies.		Optional	Required	Required	Required	Required
5	Governance Planning (Regional)						
5a	Determine requirements for, process for and extent of collaboration/cooperation among all relevant intrastate/interstate/state-federal/state-tribal/international entities.		Optional	Required	Required	Required	Required
5b	Adopt common policies and standards for the operation of PSAPs (e.g.-SOPs, accountability, reporting, etc.)		Optional	Required	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>			NG9-1-1 Implementation Maturity State				
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
5c	Develop and adopt joint 9-1-1/NG9-1-1 MOU(s) for intrastate/interstate/state-federal/state-tribal cooperation	5a	Optional	Required	Required	Required	Required
5d	Adopt and execute regional plan for system interoperability (e.g., GIS, CAD, etc.), including requirements (e.g., NIEM, standards).		Optional	Required	Required	Required	Required
5e	Develop strategic and tactical plans to be adopted by member jurisdictions.		Optional	Optional	Required	Required	Required
6	Governance Planning (Local)						
6a	Establish and execute local plan for interoperability, requirements, accountability, and reporting.		Optional	Optional	Required	Required	Required
6b	Maintain day-to-day operation of 9-1-1 system.		Required	Required	Required	Required	Required
6c	Develop and adopt an NG9-1-1 plan.		Optional	Required	Required	Required	Required
6d	Consider alignment among the SCIP(s), general 9-1-1 initiatives and the local/state/federal/tribal NG9-1-1 strategic plan(s).		Optional	Required	Required	Required	Required
6e	Develop and submit local/jurisdictional reports on 9-1-1/NG9-1-1 progress to the appropriate authority/authorities		Optional	Required	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
7	Governance Coordination (State)						
7a	Develop and adopt Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) between state and local/federal/tribal entities within the state, to achieve effective governance through partnership. Define the responsibilities of parties, scope, authority, terms, and compliance.		Optional	Required	Required	Required	Required
7b	Consider establishment of a statewide 9-1-1 entity (9-1-1 Governance Board, SIGB, SIEC, etc.) with coordination, advisory, and support responsibility for all PSAPs within the state.		Optional	Required	Required	Required	Required
7c	The statewide 9-1-1 entity is either formally (for example, defined through statute) or informally (for example, participate through subcommittees) represented on a statewide body coordinating all emergency communications, such as the Statewide Interoperability Executive Committee, Statewide Interoperability Governing Board, or the state 9-1-1 Board.		Optional	Optional	Required	Required	Required
7d	State 9-1-1 Administrator may act as liaison within and outside the 9-1-1 ecosystem.		Optional	Optional	Optional	Optional	Optional

Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
7e	Create opportunities for participation by relevant disciplines (i.e., LE, fire, EMS, emergency management, public safety communications, public safety coordination and fusion centers, public works) and coordination across technologies (LMR, broadband, cyber, 9-1-1, Alerts & Warnings, commercial wireless services) at all level of government (including tribal and Federal) on state governance body.		Optional	Required	Required	Required	Required
7f	Promote information sharing and collaboration through the utilization of a variety of mechanisms.		Optional	Optional	Optional	Required	Required
7g	Confirm an outreach and information sharing program is in place that promotes involvement from and collaboration with State-level 9-1-1 and NG9-1-1 stakeholders.		Optional	Required	Required	Required	Required
7h	State 9-1-1 Administrator provides guidance on 9-1-1 policies, funding, and operational and technical developments		Optional	Optional	Required	Required	Required
7i	Encourage SWICs, statewide broadband authorities, and 9-1-1 Administrators to collaborate.		Optional	Optional	Optional	Required	Required
7j	Optimize financial vehicles whenever possible (e.g., contracts, cooperative agreements, grants, etc.) in the acquisition of ESInet, Geographic Information Systems (GIS) capabilities, and cyber security requirements).		Optional	Required	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
8	Governance Coordination (Regional)						
8a	Develop and adopt a Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) that at a minimum, defines responsibilities of parties, scope, authority, terms, and compliance.		Optional	Required	Required	Required	Required
8b	Establish or recognize an existing regional 9-1-1 entity (9-1-1 Governance Board, SIGB, SIEC, etc.) with coordination, advisory, or support responsibility for participating PSAPs within the region		Optional	Optional	Required	Required	Required
8c	Elect/appoint permanent or rotating member to act as liaison with other governance bodies and interested parties.		Optional	Optional	Required	Required	Required
8d	Create opportunities for participation by relevant disciplines (i.e., LE, fire, EMS, emergency management, public safety communications, public safety coordination and fusion centers, SWIC, SPOC, public works) and coordination across technologies (LMR, broadband, 9-1-1, Alerts & Warnings, commercial wireless services) at all level of government.		Optional	Optional	Required	Required	Required
8e	Promote information sharing through the development and utilization of a variety of mechanisms.		Optional	Optional	Required	Required	Required

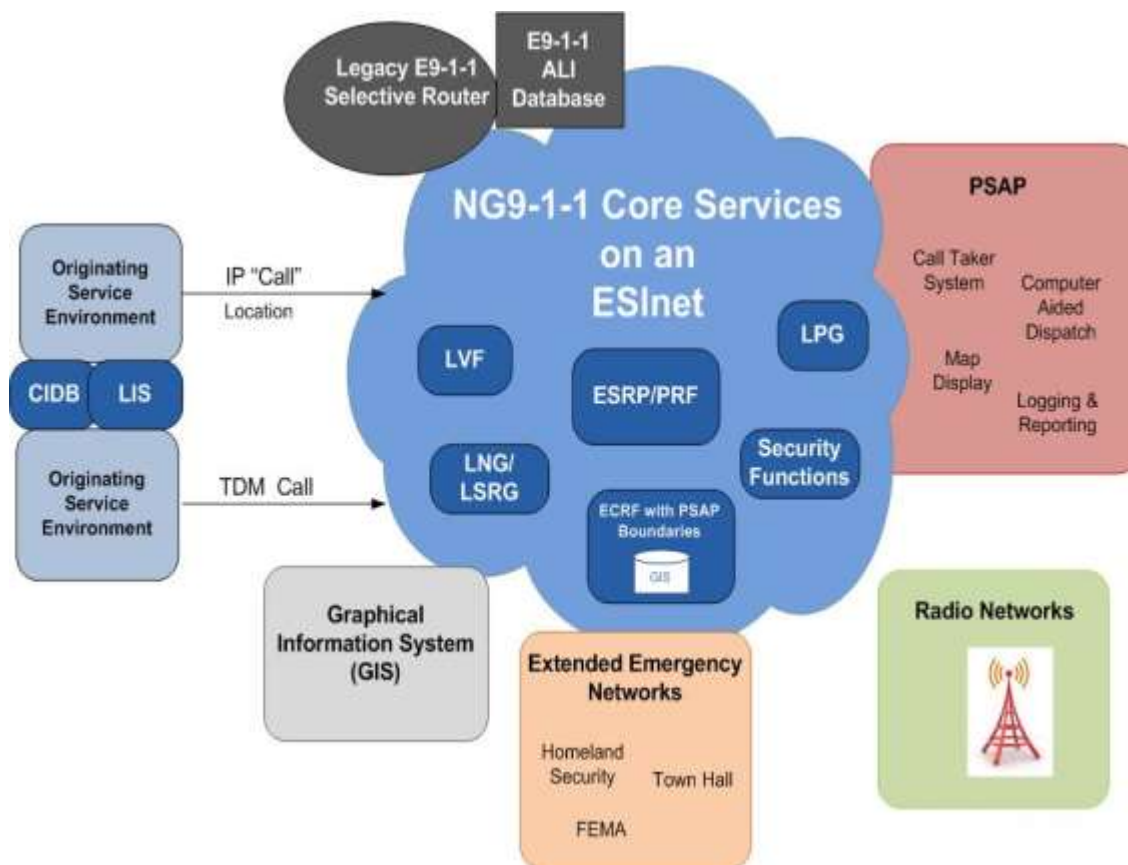
Governance Considerations Matrix							
<u>Category</u>		NG9-1-1 Implementation Maturity State					
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
8f	Confirm an outreach and information sharing program is in place that promotes involvement from and collaboration with regional-level 9-1-1 and NG9-1-1 stakeholders.		Optional	Optional	Required	Required	Required
8g	State or Local 9-1-1 Administrator provides regional governance groups with guidance on 9-1-1 policies, funding, and operational and technical developments.		Optional	Optional	Required	Required	Required
9	Governance Coordination (Local)						
9a	Draft and ratify partnership agreements (e.g., MOU, MOA), which outline the terms of partnership.		Optional	Optional	Required	Required	Required
9b	Coordinate with other local, regional, state, tribal federal public safety communications centers and PSAPs to address challenges associated with the evolving public safety and emergency communications landscape (e.g., personnel [including identity credentialing and management] , technology [including CAD and other communications resources], operations, cybersecurity, funding).		Optional	Optional	Required	Required	Required
9c	Local 9-1-1 Administrator may act as liaison within and outside the 9-1-1 ecosystem (i.e., other governance bodies, PSAPs, telecommunications industry, public safety and telephony associations, and other interested parties).		Optional	Optional	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>			NG9-1-1 Implementation Maturity State				
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
9d	Local 9-1-1 Administrator promotes information sharing and collaboration through the utilization of a variety of mechanisms on topics such as policies, funding, and operational and technical developments. Facilitate information sharing by serving on different state and regional committees and subcommittees (e.g., SIEC/SIGB, State 9-1-1 Governance Board, etc.)		Optional	Optional	Required	Required	Required
10	Governance Funding (State) & Resources						
10a	Understand the designated source of funding or shared services to support costs related to the administration of the state 9-1-1 governance body (i.e., meeting support, staff to manage logistics, financial resources to cover costs).	1a	Required	Required	Required	Required	Required
10b	Understand if participating members of the state 9-1-1 governance body do so as is part of regular duty (e.g., normal work hours, feedback on job performance to superiors, reimbursed for travel, covered by workplace insurance), or under some other arrangement.	1a	Optional	Optional	Required	Required	Required
10c	Specify if individuals on the state 9-1-1 governance body will receive compensation for serving as members (if applicable).	1a	Optional	Optional	Required	Required	Required

Governance Considerations Matrix							
<u>Category</u>			NG9-1-1 Implementation Maturity State				
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
10d	Understand authority for a state entity to collect and disburse 9-1-1 funds.	1a	Required	Required	Required	Required	Required
10e	Understand, based on statute, executive order, or regulation, state entity's tasks and responsibilities with respect to enforcing laws, rules and regulations related to 9-1-1 service and funds.	1a	Required	Required	Required	Required	Required
10f	Understand audit/oversight authority and responsibility of State 9-1-1 entity to audit PSAPs/local 9-1-1 authorities on the or other state-appropriated 9-1-1 funds (audit of surcharge funds)	1a	Required	Required	Required	Required	Required
10g	Understand if a dedicated, protected* funding mechanism is in place to address 9-1-1 operating costs and NG9-1-1 investment costs.		Required	Required	Required	Required	Required
10h	Understand the State 9-1-1 entity's role in the NG9-1-1 procurement and management process.		Optional	Required	Required	Required	Required
11	Governance Funding (Regional)						
11a	Promote economies of scale by offering the ability to negotiate a standard price for members.		Optional	Optional	Optional	Optional	Optional

Governance Considerations Matrix							
<u>Category</u>			NG9-1-1 Implementation Maturity State				
		<u>Precedent</u>	<u>Legacy</u>	<u>Foundational</u>	<u>Transitional</u>	<u>Intermediate</u>	<u>i3 End State</u>
11b	Develop a plan for resource allocation including, but not limited to centrally coordinating funding-related investment decisions and determine any potential funding methods in the region to implement solutions.		Optional	Optional	Required	Required	Required

NG9-1-1 Core Services



The use of a common NG9-1-1 Core Services system across multiple PSAPs, typically operated at either region or state level, involves a number of service system impacts and actions. Since the Core Services systems operate centrally outside the local PSAP environment, administration and management of several functions require a number of centrally responsible activities. These may be performed by one or more vendors, a combination of vendors and 9-1-1 Authority groups, or entirely by 9-1-1 Authority management groups. Examples include:

- Administration and management of inbound BCF assignments.
- Coordination, resolution, and management of GIS data feeds.
- Coordination and management of LVF operations and the provision of GIS data.
- Management of other databases that control various Core Services functional elements and their processing functions.
- Provisioning and management of the Policy Routing Function (PRF).
- Monitoring and logging of alarm messaging in the NG9-1-1 Core Services system

See the descriptions of NG9-1-1 Core Services in the 2015 TFOPA Report¹⁷. All of the above, and more, mean that one or more central database management groups may be needed to manage these processes on behalf of and in coordination with the overall PSAP population of the NG9-1-1 Core system. These are essential parts of the planning and development of NG9-1-1, whether each function is assigned to a vendor or is managed directly by the 9-1-1 Authority (who then manages the vendors actions and results).

An analysis of the expertise needed for these activities, and the related staffing and organizational structure, must be considered as part of the Governance structure. Organizations such as NENA are involved in the development of documents related to management of NG9-1-1 services and systems. Stakeholders are encourage to remain abreast of their progress.

4.2 OSP Access to NG9-1-1 Systems

The eventual access to deliver calls and data (of all types, voice, text, pictures, video) is by electronically consulting a national Forest Guide to identify each individual state or sub-state level NG9-1-1 system and its logical network access points. In the meantime, there will be a number of transitional and optional ways to guide calls to those points, for further routing by the NG9-1-1 Core Services to appropriate PSAPs within the NG9-1-1 systems. The National Forest Guide methods were described in the first TFOPA report, in 2015.¹⁸

This section of the second TFOPA report, also about planning to optimize the overall NG9-1-1 service process, including PSAP configurations, covers the major choices and options for access by the Originating Service Environment (OSE) and how those relate to 9-1-1 Authority planning and preparation for NG9-1-1.

The starting point for 9-1-1 access is to establish interconnection at a point of interface to the current 9-1-1 system. A point of interface is a formally recognized demarcation point between those originating 9-1-1 requests for service and those servicing such requests. Those originating these requests are responsible for their side of this demarcation point and 9-1-1 authorities have the responsibility for the other side. It is important to note that definition and ongoing usage of such demarcation points are subject to policy and cost considerations that go beyond simple technology issues. The interconnection of specific originating switches, either legacy or soft-switches, and technology associated with internet based services (such as VoIP), telematics, large MLTS or alternate service providers¹⁹ utilize these demarcation points to access the routing switches in E9-1-1 systems or to equivalent SBC points in pre-NG9-1-1 systems (IP based, but not using true NG9-1-1 architecture functions).

In some specialized cases, where the service territory of wireline originating switch lies entirely within a single PSAP's jurisdiction, there may have been direct connection to the PSAP equipment. As referred to above, the evolution of the current state of affairs in access to 9-1-1 systems was directly tied to cost factors and funding, and the regulatory environment involved, and has attendant limitations for functions otherwise provided by the Selective Routing switch and other E9-1-1 features. The advent of number portability and mobile service complicated these originally simple arrangements. There has been recent evolution in some areas to transitional NG9-1-1 systems, where the OSE providers connect using an IP conversion into the transitional NG9-1-1 systems. Transitional 9-1-1 systems often accommodate all of the above connection types to ensure interoperability and support a variety of OSP connections.

¹⁷ TFOPA, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf.

¹⁸ TFOPA, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf.

¹⁹ These include SPs where mobile handsets interact with non-carrier servers, which in turn interconnect with the Core 9-1-1 service systems

By and large, there is a mixture of OSE direct trunking to the front end of the various central 9-1-1 systems, and aggregation by intermediate connectivity providers to the same ingress points for wider service areas for a given OSE entity. Such an aggregator often services multiple OSP's, which may not be individually known or detectable by the 9-1-1 Authority or PSAPs. Note that these connections are typically segmented by state boundaries due to regulatory and traditional reasons. Even where a multi-state E9-1-1 or transitional NG9-1-1 common system is employed, OSE inbound trunk connectivity is usually still state segmented.

With the advent of IP connectivity, larger scale OSE networks, and the trend toward regional or state-wide NG9-1-1 plans, an opportunity was foreseen to simplify originating networks and lower overall costs for both the OSE stakeholders and for NG9-1-1 service systems. While such plans will have to maintain redundancy and reliability, and to a degree duplication, moving to logical networks utilizing IP protocols can, over time, vastly lower costs and maximize networking efficiency nationwide. This evolution is complicated by current laws, regulations, local and corporate priorities and preferences, and uncertainty in how to plan and prepare to accomplish the task. The transition of the PSTN to IP structures is a major factor in driving these lower costs and greater efficiencies. Foresight and the readiness of Public Safety to provide the features in NG9-1-1 which enable these overall changes is also necessary.

It is important to note that “access to NG9-1-1” has two parts, access by OSEs and access by PSAPs. It is important, as well, to note that the intervening “NG9-1-1 systems” provide the all-important interconnection between OSEs and PSAPS for the purposes of emergency communications. As such, access to NG9-1-1 systems “on both ends” is key to the correct functioning of the entire system. It does no good for OSEs to have access to the system if PSAPs, the intended recipients of information from OSE customers, cannot consistently and affordably access NG9-1-1 systems.

4.3 ESInet

The following bullets represent concepts that should be considered prior to the establishment of an ESInet:

- Understand the defined term ESInet (what it is and its role)
- Size the ESInet relative to its purpose over time
- Design the ESInet with appropriate resilience, quality and SLAs upfront
- Ensure proper network management and security at each stage of its evolution
- Anticipate cross entity collaboration

The NENA i3 model is based on the concept of an Emergency Services IP Network (ESInet) as a foundational element of a NG9-1-1 “solution”. However, its value cannot be fully realized until the agency begins layering on applications and services. Typically, this will initially consist of Transitional 9-1-1 elements that will evolve to NG Core Services. At the most rudimentary level, NG9-1-1 cannot occur until an ESInet is instituted for the Public Safety entities that will support the processing of emergency service requests. It is comprised of the Physical Layer transport used for the routing of data to/from and amongst those interconnected. The network must support IP and it can be established using any access technology. For clarity, the reader should understand that as presented here and defined in the NENA i3 specifications, the ESInet is separate from / does NOT include any of the NG9-1-1 Core Services, such as the ECRF, ESRP, LVF and LIS.

This document is intended to identify primary considerations of those implementing an ESInet. It is not intended to be a comprehensive guide or detailed technical reference. That type of information is available from NENA²⁰ and internetworking bodies, such as CSRIC²¹ and ATIS/ESIF²².

4.4 Security

Provisions must be made to secure the network and NGCS, as they are not considered to be a “walled-garden” or isolated network free from outside interaction. While the use of redundant private Multiprotocol Label Switching (MPLS) networks lends to the necessary reliability of data transmission across the ESInet, it would not mitigate the possible impacts to overall network security. The 9-1-1 Authority, representative of prospective interconnected PSAPs, should verify the inherent network security capabilities of all providers who would build networks to constitute its ESInet. Also for consideration is the fact that any device that could generate an emergency service request to an interconnected PSAP would reside outside of the ESInet. Therefore, all calls should traverse a Border Control Function (BCF) prior to entering the network. The use of session border controllers and firewalls on the edge of the ESInet is a recommended best practice by NENA, so as to minimize the potential for attacks and/or intrusions from external networks.

Each 9-1-1 Authority or collection of PSAPs that implements an ESInet should have Virtual Local Area Networks (VLANs) across each of the separate, redundant and diverse IP networks. This is consistent with the best practice recommended in NENA’s Network Information Document (NID) on ESInet design which states, “The PSAPs should use redundant local area networks for reliability.”

Other ESInet security items for consideration included the use of IP Security (IPsec) for encryption on the transport, specific firewall and router policies, and the isolation of applications running on the ESInet from public internet connectivity.

4.4.1 Identification/Discovery

The primary foundation of effective cybersecurity is the identification of the information assets; hardware, software, products tools, and systems within the organization. Categorize the information systems and the information processed, stored, and transmitted by that system based on an impact analysis.

1. Inventory all existing systems and applications - Create an inventory/register of the information assets requiring protection. It is important that the asset inventory/register is reasonably complete to ensure thorough protection.
2. Classify the assets - Every asset needs to be classified according to the criticality of the asset to the organization. This information is used to determine the appropriate level of controls to apply.
3. Identify owners - All information assets are managed at organization level. Individuals are assigned and made responsible and accountable for the information assets. Specific individuals

²⁰ NENA, <https://www.nena.org/?page=Standards>.

²¹ FCC, Communications Security, Reliability and Interoperability Council, <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-1>.

²² ATIS, <https://www.atis.org/>.

are assigned with the ownership / custodianship / operational usage and support rights of the information assets.

4. Identify applicable laws, regulations, and customer requirements. Those requirements should then be placed against the other controls that exist to identify and document the controls in place to meet the requirements.
5. Discover existing vulnerabilities - Vulnerabilities can exist in the form of an unpatched system, an unidentified software bug, or a poorly implemented control. Scanning tools are used to identify vulnerabilities within an organization's network. Resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases are available to identify flaws discovered in organizational information systems. Audits and incident management programs identify necessary control improvements.

4.4.2 Assess/Prioritize

The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the security controls necessary to protect the individuals, operations and assets of the organization. This phase establishes the security controls for the information system based on its categorization, assessment of risk, and local conditions.

1. Conduct risk assessments - Identify and quantify the risks to the organization's information assets. This information is used to determine how best to mitigate those risks and effectively preserve the organization's mission.
2. Establish security controls - Using the output of the risk assessments, vulnerability management data, and information security requirements establish the correct security controls for the environment.
3. Develop remediation plans - Taking into account the level of risk, plans are developed to perform the remediation of the threats or vulnerabilities facing an organization's systems. The plan includes options to remove threats and vulnerabilities and priorities for performing the remediation.
4. Prioritize execution - Use the prioritized and collected data to execute remediation plans, mitigate vulnerabilities, and improve controls.

4.4.3 Implement/Operate

This stage is focused on the application of identified and applicable security controls adhering to all relevant laws, regulations, and customer requirements. It involves the people, processes and technology for the secure operation of information systems in accordance with the acceptable level of organizational risk.

1. Documentation - Documentation of the policies, procedures, and controls are necessary to ensure completeness, facilitate training, and measure effectiveness. This documentation is subject to regular update and revision as information security must adapt to changes in both organization (participants) and the external environment (systems/assets).
2. Administer additional security controls

- a. Access Control - The identification of authorized users of the information system and the specification of access privileges reflects the requirements. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. This includes removal and periodic review of access rights.
- b. Awareness and Training - The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.
- c. Audit and Accountability - Audit review, analysis, and reporting covers information security-related auditing including auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP.
- d. Configuration Management - Baseline configurations for information systems and system components including communications and connectivity-related aspects of systems are identified. They are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components, network topology, and the logical placement of those components within the system architecture.
- e. Contingency Planning, BCP/DR, Continuity of Operations - Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired.
- f. Identification and Authentication - Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users.
- g. Incident Response - Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk owner.

- h. Maintenance - The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements, approves and monitors all maintenance activities, and checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
- i. Media Protection - Controls are in place to protect electronic and physical media while at rest, stored, or actively being accessed according to the classification of the information. Electronic media includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. Physical media includes printed documents and imagery.
- j. Personnel Security - Personnel security involves the controls to address the risk related to the confidentiality, integrity and availability of information accessed in individual job roles. Consideration is also given to employee termination and transfer. Access agreements provide an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.
- k. Physical and Environmental Protection - Physical and environmental protection includes consideration of controls for the security of power equipment and cabling, temperature and humidity controls, and emergency power, lighting, and shutoff. Facility and system access are granted to only authorized individuals and involve regular access rights reviews.
- l. Planning - Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements.
- m. Program Management - Information security program management is the governance of designing, implementing and improving security practices to protect critical business processes and assets across the organization.
- n. Risk Assessment - A risk management program entails identification of key assets whose loss would negatively impact the organization, vulnerabilities and threats to those key assets, and decisions on addressing vulnerabilities, risks, and threats.
- o. Security Assessment and Authorization - The development a security plan to assess the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements. Security authorizations are official management decisions, conveyed through authorization decision documents, by senior management to authorize the operation of information systems and to accept the risk based on the implementation of agreed-upon security controls.

- p. System and Services Acquisition - Requirements analysis is the primary focus of system and services acquisition to provide the assurance that all security considerations will be integrated into all phases of the system lifecycle. The security plan provides a complete description of the information system, and security test plans are developed for verification of correct implementation and effectiveness.
 - q. System and Communications Protection - Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security. Subnetworks that are physically or logically separated from internal networks, demilitarized zones or DMZs. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements.
 - r. System and Information Integrity - Controls to ensure the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures are a primary objective. Information integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance the information has not been altered.
- 3. Execute remediation plans - This stage is the execution of the plans for remediation based on the criticality of the asset to the organization. This is the result of risk assessment analysis, vulnerability management, and other input data to ensure the best approach at improving the security posture.
 - 4. Requirements Conformance - Controls to ensure the compliance with all laws, regulations and contractual agreements must be in place.

4.4.4 Monitor and Evaluate

The intention of this phase is to examine and analyze the operational environment and to report on the security state of the organization. The purpose of the assessment is to determine if controls are implemented adequately, operating appropriately and as intended with the desired outcome.

- 1. Baseline the current environment - Knowledge of the current environment is necessary for incident detection.
- 2. Event logging - Capturing the events within the organization's environment is necessary for incident investigation.
- 3. Capture metrics - Metrics are used to determine if objectives of the organization are being met and where improvements can be made.
- 4. Compliance evaluation - This includes the verification of adherence to all laws, regulations, and contractual agreements.
- 5. Control effectiveness - This stage evaluates each control to ensure it is working as intended through audit information, manual, and/or automated tools.

4.4.5 Test/Evaluate

1. Audits - This includes the verification of adherence to all laws, regulations, and contractual agreements.
2. Control effectiveness - This stage evaluates each control to ensure it is working as intended through audit information, manual, and/or automated tools.
3. Contingency plans, BCP/DR - Business continuity and disaster recovery plans need to be evaluated regularly for updates and for testing to validate plans.

4.4.6 Improve/Evolve

Based on output from the previous phase, the organization can make informed decisions on the suitability of implementing new controls or changing existing controls to continually improve the security posture. Identification of areas of improvement and best practices is essential. Focus is given to security training and awareness allowing the organization to continue to evolve.

1. Reassess - As data related to the information security program is gathered and provided it is important to reassess the policies, procedures, and controls in light of all new information provided. This information should be made available to executive management for improved decision making.
2. Re-evaluate - Information security management is constantly evolving as major changes occur that would require another evaluation of the security management program. Some of these major changes include security incidents, organizational structure, business or technology changes and resources. As information technology shifts, it is imperative to re-evaluate and improve the security of mission-critical systems.
3. Training/Awareness - Security awareness and training is an important part of an information security program. The organization's requirements for the awareness and training program need to be clearly defined and resourced. Topics documented within the awareness and training program policy should include roles and responsibilities, development of program strategy and a program plan, implementation of the program plan, and maintenance of the awareness and training program. Using multiple channels of communication can increase the effectiveness of the program.
4. Short/long term capacity planning - Ensure systems are sized appropriately based on data gathered in re-assessments and re-evaluation. Do the existing systems handle the increased capacity during an event? As systems have evolved the question is do the original security measures handle the new capacity from either unexpected growth or additional functions added after initial deployment. Capacities could include but are not limited to throughput, interfaces, processing power, storage size, etc. For example storage size, ensure the space allotted for logging or system backups is adequate. Specifically on logging storage capacity, a concern may be during a large scale incident if the log space is undersized systems may start to overwrite themselves, if out of space systems possibly fail as they cannot make entries in to logs, etc.

4.5 Sizing

It is imperative, that a NGCS provider, PSAP, or Public Safety Entity connecting to the ESInet properly size its access bandwidth to account for the multimedia it is expected to exchange. This includes not only

the initial design requirements but ongoing capacity management too as the requirements should be expected to change over time.

4.6 Resiliency, Quality and Service Levels

An ESInet solution that utilizes redundant and diverse IP/MPLS networks for reliability and availability is defined in the i3 spec.²³ Use of label switching in MPLS provides for connection-oriented virtual circuits, over which data can traverse the ESInet. The MPLS networks should be configured to allow for the definition of different quality of service (QoS) levels for data being transmitted. The importance of such a capability is evident when one considers that industry standards could recommend real-time voice traffic be given a higher priority across the network than still pictures, for example. Thus, the ESInet provider will be able to designate different multimedia destined for the PSAPs with different QoS as applicable, for prioritization across the networks.

4.7 Network Management

Monitoring, surveillance, alarming and technical support of the ESInet is another key consideration. The ability to surveil the underlying IP networks that form the ESInet, receive real time actionable intelligence of its operating condition is paramount to the service delivery of these mission critical networks. Ideally, this network management is systematically correlated across the separate redundant and diverse MPLS networks so that while the networks may operate independently for greater resiliency they can be managed as one network “solution”.

4.8 Cross Entity Interconnections and Operations

It is expected that the ESInet will be deployed on a multi-county, regional basis at a minimum, with statewide and even nationwide implementations possible. To take full advantage of the capabilities of these NG9-1-1 systems, the interconnected PSAPs will want to establish any necessary agreements required to allow for the sharing of data between the entities, as the IP network will make possible the seamless transfer of calls and data. This is an operational consideration for the PSAPs, and it isn't typically prevalent in legacy E9-1-1 operations. However, it will prove beneficial to all those involved if the existing operational obstacles that make data sharing difficult between disparate PSAPs are negated, as the technology that allows for the ease of sharing is implemented.

4.9 NG9-1-1 Operational Impacts

Deciding what resources will be shared and how the work of PSAPs will utilize the shared resources has important implications for how the public's need for 9-1-1 service will be met. It will also affect the PSAP Telecommunicators who are held responsible for handling 9-1-1 calls from the community.

Use of a common NG9-1-1 Core Services system across multiple PSAPs, typically operated at either regional or state level, involves a number of service impacts and actions. Since the NGCS operate centrally outside the local PSAP environment, administration and management of several functions require a number of central responsible activities. These may be performed by one or more vendors, vendors and 9-1-1 Authorities, or entirely by 9-1-1 Authorities.

Examples include:

- Administration and management of inbound BCF assignments, including determination of OSE entities providing calls/messages and data on specific ingress paths.

²³ NENA, <https://www.nena.org/?page=Standards>.

- Coordination, resolution, and management of GIS data feeds from individual PSAPs or other authoritative data sources. GIS data management functions include resolution of gaps, overlaps and measuring overall GIS accuracy and currency.
- Coordination and management of LVF operations, and the provision of GIS data for validation purposes. Actions will vary depending on whether the LVF process is a service provided within the Core Services by an NG9-1-1 Core operating vendor or the 9-1-1 Authority, or is operated by individual OSE entities or a 3rd party provider to OSE entities. In any case, the 9-1-1 Authority with responsibility for NG9-1-1 Core Service operations has responsibility to see that the process works effectively.
- Management of other databases that control various NGCS functional elements and their processing functions such as user roles and access management.
- A major consideration is the management of the Policy Routing Function (PRF) which is used to control alternate routing, the distribution of calls for PSAP overflow or out-of-service conditions, the automatic acquisition of selected additional data during an emergency call, and potential call delivery modification (to another PSAP or to specific TC positions) based on type of call (text, voice or video). The design of the i3 architecture also includes the PRF automatically sensing PSAP delivery channel or PSAP equipment status, with the appropriate i3 compliant software at the PSAP, and making pre-defined and authorized changes in call routing.
- Logging and alarm messaging in the NGCS system must be managed, reacted to, and resolved.

See the descriptions of NG9-1-1 Core Services above. All of the above, and more, mean that one or more central database management groups may be needed to manage these processes on behalf of the overall PSAP population of the NG9-1-1 Core system. These are essential parts of the planning and development of NG9-1-1, whether each function is assigned to a vendor or is managed directly by the Authority (who also manages any vendor actions and results). An analysis of the expertise needed for these activities, and the related staffing and organizational structure, must be considered as part of the Governance structure.

4.9.1.1 Monitoring and Managing

Establishing uniform methods of interaction, interoperability and collaboration is critical for effective system monitoring and rapid system restoration in times of impairment. As transition towards NG9-1-1 proceeds, it becomes harder to identify the basic operational responsibilities of 9-1-1 Service Providers (e.g., routing the 9-1-1 call, providing mechanisms to control abnormal routing needs, maintaining and housing GIS and other 9-1-1 data, managing location validation processes, network connectivity, network and data system monitoring and troubleshooting), and those of the PSAP CPE. The elements are complex, new, continually evolving and assembled in many different ways based on circumstances, specific needs and constraints.

Monitoring occurs at various touch points and should be coordinated for maximum benefit. OSPs must monitor their networks and facilities to ensure they are in good working order and availability has not been compromised. OSPs must have working relationships with each 9-1-1 Service Provider for reporting, trouble shooting and managing service disruptions that occur in their networks or impacts they can observe occurring in the 9-1-1 Authorities domain. These relationships manifest themselves in

communications between Network Operations Centers and/or service operations centers. Every OSP and 9-1-1 Service Provider has the responsibility for using appropriately designed systems and for monitoring its own systems and services to detect and respond to 9-1-1 service-related impairments and participate in appropriate situational awareness. Similarly, for their owned or controlled systems, every PSAP and/or 9-1-1 Authority has the responsibility of monitoring its own systems and services to detect and respond to 9-1-1 service impairments and participate in appropriate situational awareness. It can be extremely complex to monitor and respond to impairments within individual networks. OSPs, 9-1-1 Service Providers and PSAPs should implement a secure information sharing system that facilitates sharing of observed network impairment issues and the ability for individual system providers to notify appropriate parties at the onset of an impairment.

Because of the connected nature of 9-1-1 systems, a service impairment in one system is likely to create a service impairment or be observable in another part of the ecosystem. Effective trouble shooting and service restoration requires communication and coordination across all entities involved. During 9-1-1 service impairments, system capabilities are always restored at some point in time, with partial or full recovery and resolution. Resolution of the impairment must be effectively communicated to each stakeholder. Information sharing should include both periodic updates and final resolution (preferably with a root-cause analysis that allows all parties to learn from impairment). Timely conveyance of system impairment resolution also allows providers who have invoked alternate service architectures to return to normal operating procedures.

4.9.1.2 PSAP Operations

PSAP operations have historically been unique to each PSAP, and driven by the needs of the agencies they serve and the individual agencies actively participate in defining the operational procedures specific to that agency. The more agencies served by a single PSAP the more complex the operational procedures become. However, it is important to note that as NG9-1-1 efficiencies are gained with optimized networks and core services, the melding of standardized operating procedures will need to be accomplished. Through cooperation and partnerships with multiple agencies a detailed comparison of existing policies and procedures will be required, as well as careful consideration should be given to how all changes could affect PSAP service requirements. Part of this comparison must include examination of the roles and responsibilities of the Telecommunicator, and modify roles, where appropriate, to ensure the successful fulfillment of their assigned duties.

9-1-1 jurisdictions currently have procedures and processes in place to deploy, manage and maintain E9-1-1 systems, and their interactions with vendors, especially a 9-1-1 service provider. As PSAPs migrate to NG9-1-1 those procedures and processes may need to evolve to support the next generation environment.

4.9.2 Operational Aspects of NG9-1-1

Before implementing NG9-1-1, it is highly recommended that a Project Implementation Plan be created. This plan should include, but is not limited to, the following elements:

1. Name a Project Manager to handle the development and implementation of the Plan.
 - a. Beyond the Project Manager, the project needs a team of PSAP Managers, CAD, GIS and IT representatives (that are familiar with 9-1-1 GIS which requires a higher level of accuracy than most GIS business operations) to assist the Project Manager in managing the ongoing planning and deployment of the NG9-1-1 system. Depending

on the size of the project local 9-1-1 authorities should consider full-time or contracted services to support the Project Management demands.

- b. This position should be responsible for documenting the progress, knowing the stakeholders that need to be involved in making decisions, able to implement the plan, organize schedules and deadlines, deal with project updates, implement strategies, and in general the overall delivery of the project. This position should have project management and facilitation skills, political and legislative skills, and possess knowledge specific to 9-1-1 CAD/GIS/ IT Support. The team must be able to make recommendations about how to implement the system. This team assignment will be long term regardless of whether the planning team elects to choose someone in-house or an outside consultant group that specializes in CAD and NG9-1-1.
2. In areas where PSAPs are required to have a 9-1-1 Plan by statute or regulation, it will likely be necessary to update that Plan. It will be important to identify the necessary changes and go through the process of updating the plan. Some 9-1-1 Authorities are responsible for setting the Plan, or it may fall under the PSAP Managers responsibility. Either way, the PSAP Manager should consult with the 9-1-1 Authority to ensure the Plan will be in compliance with the changes to IP network and NG9-1-1 deployment.
3. Identify all operational impacts for the PSAP, which includes the impacts the transition to NG9-1-1 will have on PSAP operations and staff.
 - a. Identify needs for additional staffing. Those staffing needs may include additional IT staff to manage and mitigate the system which includes permissions, alarms, maintenance, etc. There is a possibility of increased volumes of Freedom of Information Act (FOIA) requests and additional requests for court testimony as the Holder of the Record. Also, consult state and local laws or rules regarding the chain of custody for evidence.
 - b. Some deployments, such as the hybrid approach, will require the cooperation of all the affected PSAP managers in making decisions that will impact their operations on a global level or independent to their PSAP.
 - Memorandums of Understanding and other agreements should be worked out with all agencies involved.
 - Identify who will be responsible for the technical and maintenance needs for the system and how the cost sharing will be handled.
 - Determine what type of alarm monitoring the system will need and how those notifications will occur. This may be something that the network vendor provides, but it may also be something that a third party vendor provides. Once determined, set up notification processes that identify appropriate groups, and contacts. Developing a centralized contact list allows all stakeholders to be notified and will be prepared for reacting and responding to the alarms.

4.9.3 Technical Considerations

Technical considerations will need to be assessed, and operational procedures will need to be created before the implementation of the NG9-1-1 system. Examples of some operational impacts are as follows:

1. Trouble notifications for new systems and functions
2. Evacuation plan and back-up PSAP changes
3. Emergency notifications for system issues
4. Changes in reporting ALI discrepancies
5. How to use new technology (text, MMS, RRT, video calls, etc.)
 - a. How to push data out to responders and other agencies
 - b. Security of the data and transport
6. ANI/ALI screen changes
 - a. Additional data fields
 - b. How to use the new data that gets delivered
7. Overflow or reflow routing plans and ability to change those on the fly
 - a. See discussion of PRF capabilities and management
8. Scenario based routing plans – what they are for and how they work
9. How to deal with address (MSAG/GIS routing) fallout issues.
10. Call handling for new technology (text, MMS, RTT, video calls, etc.)
11. Call transfers

4.9.4 Processing System Alarms

In general, 9-1-1 Authorities and PSAPs who have implemented Transitional NG9-1-1 have not been completely prepared for the alarm processing aspects of IP and NG Core Services deployment. It is imperative that someone or multiple persons be identified to monitor and manage the system alarms. There must be a thorough training for those handling these functions. The following items will need to be determined as well.

1. Who monitors which alarms?
2. What is the role of the PSAP IT staff?
3. Plan and train for Alarm Codes and understand what each of the alarms mean?

- a. Is the alarm something that needs to be addressed? If not, what should you be looking for?
4. Identify the Network and Core Services provider's responsibilities in dealing with the alarms?
5. Determine if new system components for alarm management are needed.
6. Is there an expense to monitor alarms?²⁴

4.9.5 Data Management

The transition to NG9-1-1 technologies assumes that PSAPs are likely starting with an environment consisting of traditional E9-1-1 components, such as an ALI system, selective router(s), a Database Management System (DBMS), tabular MSAG, and a legacy 9-1-1 network. It also assumes that PSAPs have developed a set of GIS data to a level of accuracy that approximates the contents of the tabular MSAG. Furthermore, it assumes that PSAPs and/or 9-1-1 Authorities that are using GIS have previously performed preliminary reconciliation between their GIS data and their MSAGs. This is essential to provision the NG9-1-1 technology GIS based Location Validation Function (LVF) and Emergency Call Routing Function (ECRF). If this is not the case, the preparatory work for PSAPs and/or 9-1-1 Authorities to implement NG9-1-1 services will be substantially lengthened as the technology is dependent upon the following minimum foundational GIS elements:

- a. Street/Road centerlines with address ranges
- b. Address points
- c. PSAP boundaries
- d. Emergency service zone boundaries (combined fire, law, and EMS)
- e. Fire response boundaries
- f. EMS response boundaries
- g. Law enforcement response boundaries
- h. Authoritative boundaries (represents area of responsibility for each GIS agency)

Until such time that the industry and/or Federal/State Government have established Location Information Servers (LIS) and Customer Information Data Bases (CIDBs) on a larger regional scale, the 9-1-1 authorities should gather and maintain the GIS data necessary to support their respective jurisdictions. They should do so in conformance with open standards, coordinating with surrounding jurisdictions, to the highest regional level available, ideally into a centrally managed data repository.

²⁴ In a multi-node situation, 9-1-1 Authorities will likely want to purchase an alarm monitoring module to view the alarms ahead of time.

4.9.5.1 Geographic Information System (GIS) Routing and Data

The MSAG/GIS routing changes will need to be handled differently during Transitional, Intermediate, and End State NG9-1-1 deployments. It will be necessary to determine how to manage gaps and overlaps in the GIS data as the process will be different under NG9-1-1.

The NENA standards for GIS Data accuracy recommend a minimum of 98% accuracy from a GIS centerline or an address point file. The GIS datasets in NG9-1-1 will now be used to validate telephone subscriber addresses before a 9-1-1 call is placed and will also be used to route live 9-1-1 calls to the proper PSAP at the time of the call. With GIS functioning as the foundation of the NG9-1-1 system, the importance of data accuracy cannot be overstated. The process of building, collecting, cleaning and maintaining a GIS database is complicated and labor intensive. The QA/QC aspect of GIS maintenance is also crucial but often missed or rarely performed. Parties responsible for GIS accuracy must ensure that protocols and practices are in place for handling specific updates. Early in the process, decisions will need to be made or coordinated with appropriate vendors and partnering agencies regarding items such as data format and if the NG9-1-1 is operating from a GIS centerline or an address point file.

4.9.5.2 MSAG / ALI

It is important to understand that migration to NG9-1-1 will result in data format changes. In the legacy environment, the ALI server can only deliver 512 characters to the PSAP. That limits the total number of fields displayed on the 9-1-1 screen. NG9-1-1 providers will be able to deliver a much larger data stream and opens up a multitude of fields that can now be displayed to the Telecommunicator. It will be necessary for the PSAP Manager to determine what fields to display and ensure the creation of SOPs to correlate with the changes and training for those handling the calls. With ANI/ALI data format changes, it will be imperative that the PSAP Manager works with their CAD, CPE, Logging Recorder and Supplemental Information Application vendors to ensure the data format changes work with those systems appropriately.

It is important to know what the legacy ALI provider will require on their end for the switch over, timeline, notifications, and disconnection. This discussion must take place with both the NGCS and CPE vendors.

4.9.6 NG9-1-1 Implementation Planning

NG9-1-1 Planning requires the establishment of a strategic plan. Within the strategic plan are specific project prerequisites (e.g., critical path dependencies) that need to be clearly defined before the project begins. Some of those key factors include; NGCS elements and databases, ESInet implementation, GIS and PSAP sub-systems such as CAD. Planning must also include consideration of costs associated with project timing and delays. Project management best practices should be considered and include a list of risk factors and mitigation strategies that may be implemented to address and overcome the risks.

Additional planning items that need to be clearly defined during the preplanning phase include:

1. Developing a list of required tasks for go-live and a prioritized list of staffing dependencies and tasks assignments for the actual cut-over.
2. GIS items to be completed such as the currency of centerline, MSAG updates, and ALI data at a 98% accuracy level which is recommended by NENA.
3. Other databases within NG9-1-1 Core services must be planned, populated and tested.

4. Ensuring that the primary and secondary network infrastructure is built out, tested and ready before cut-over.
5. Ensure there is a tested plan in place for Disaster Recovery.
6. Conduct weekly, then daily status meetings as needed as the go-live date approaches. Those in attendance should include 9-1-1 Authority representation, PSAP Directors or Managers, Technology team members, Project Managers, Consultants, Network and Core Services Providers and representatives of all agencies using the PSAPs services..
7. Third Party subject matter experts to verify the network infrastructure and critical interfaces are in place and operating accordingly.
8. The Project Management Team should track budget, resources, and timeline for all involved parties and manage the deliverables for the project.
9. Monitoring for and management of scope creep through the use of check lists.

Upon NG9-1-1 preplanning phase completion, the project management team will need to ensure the following items are examined and included in the implementation phase:

1. Notify PSAPs of upcoming changes that include their schedules, training, and documentation of changes to the operations.
2. Work with the Originating Service Providers (OSPs) for all upcoming changes which could include network demarcation changes and data requirements.
3. Create a communication plan for the public safety agencies, and business partners served by the PSAP to include:
 - a. Upcoming changes impacting the PSAP functionality
 - b. New features and functions
 - c. Schedule of events
 - d. System downtime potential and operational impacts
 - e. Contingency plans
4. Create new Standard Operating Procedures (SOPs) for all operational and technical function changes.

NOTE: There will need to be considerable thought and planning placed into the update and addition of operational SOPs, followed closely by addressing the need to train PSAP staff. Several key items for consideration are listed below:

- a. Changes to CPE Equipment and how to use it

- b. Recording and Logging
 - c. New technology
 - d. New responsibilities
5. PSAPs need to understand that audio will "sound" different in the new environment versus what they are used to receiving in the legacy analog world. In the new IP environment, there may be no background sounds at all. It will be important to work with the service provider to understand the difference.
 6. ALI connectivity and data delivered may change depending on the service provider. It will be important to work with the NG9-1-1 service provider to understand any ALI management differences.
 7. Supervisors and managers may need to know how to dynamically route and reroute call flow to other PSAPs.
 8. Create and schedule training for all PSAP staff and verify training accuracy and completeness.
 9. It is essential that the 9-1-1 Authority and PSAP Manager have the appropriate level of knowledge needed to understand, plan, promulgate and manage the IP deployment. Having proven subject matter experts involved are critical to the success of the project.
 10. Development of a public education plan for the general public is needed. The plan should include education on the benefits of the advanced NG9-1-1 system.
 11. Schedule Go-Live, ensuring all technical staff will be on-site the day of the cut-over.
 12. Go-Live
 13. The Project Management Team will need to transition into a review committee structure to evaluate the day to day operations of the new system which includes needed enhancements, training, and other operational concerns.
 14. Ongoing Operational Review.

4.10 Staffing and Training

4.10.1 Introduction

Since the inception of 9-1-1 in the United States in 1968, technology has advanced the roles and responsibilities of 9-1-1 telecommunicators. The public safety telecommunicator's position has transformed from a clerical staff handling telephone calls and incidents with manual methods, to technically savvy protective service professionals managing multiple integrated technology systems to track and manage public safety field resources and responses. The public safety telecommunicator position will continue its evolution with the integration of Next Generation 9-1-1 technologies.

Any 9-1-1 Authority transitioning to NG9-1-1 may find staffing and training to be one of their most challenging tasks, second only to the increased budget and funding needed for infrastructure. As technology evolves, systems have become more advanced and new skills are needed to perform a public safety telecommunicator's job effectively. Today, public safety telecommunicators are required to operate a sophisticated work station comprised of multiple networked computer and technology systems. Concurrently, the public safety telecommunicator must be able to quickly answer, elicit pertinent information from a distraught caller, analyze given information, and expediently make appropriate entries into various technology systems. Additionally, in many jurisdictions public safety telecommunicators are required to be licensed or certified, hold State Criminal Justice Information System and Federal Bureau of Investigation National Crime Information Center access permissions and also be certified emergency medical dispatchers. In many jurisdictions, oftentimes public safety telecommunicators need certifications in cardiopulmonary resuscitation (CPR) and in automated external defibrillation (AED).

While the public safety community is entrenched in defining, developing, and deploying NG9-1-1 technologies that promise to revolutionize the way that PSAPs receive and process citizen's calls, the ability to hire, train, and retain qualified public safety telecommunicators has become a nearly insurmountable challenge. Low pay, long work days, constantly evolving technology, very high stress where errors can be deadly, all contribute to the difficulty of recruiting and retaining qualified telecommunicators. Some in the industry believe that as NG9-1-1 technologies become available and virtually put the public safety telecommunicator in the incident scene itself, the difficulties of hiring and retaining qualified people may dramatically increase²⁵. The onset of NG9-1-1 technologies will also require 9-1-1 authorities to consider the hiring of additional staff to fulfill requirements not present in current systems.

Training currently given to telecommunicators around the country varies widely among PSAPs. Standards related to personnel and training exist,²⁶ but have not been implemented on a national level. Many States have enacted their own laws or ordinances to govern minimum staffing levels, training and qualifications. Additionally, there are some number of PSAPs which operate using best practices or guidelines based on available funding for both staffing levels and training considerations. Unfortunately, many of the documented standards that exist for staffing calculations, which are relatively comprehensive, may not sufficiently address the additional data elements that are necessary to determine future technological processes in NG9-1-1.²⁷ These new data elements, for example, may include the length of time to process new and more complicated incident types and how other administrative and support positions fit into the staffing formulas.

Operational mistakes produced by human error resulting from problems with new technology, stressful working environments and a focus of the emotional and quality of life issues of the telecommunicators need to be taken into consideration.

Staffing impacts may include:

- a. Freedom Of Information Act (FOIA) increase.
- b. Court testimony for Holder of the Record agreements may increase.

²⁵ It is not known to the authors the magnitude with this view, but the Working Group believes it would be valuable to determine.

²⁶ NENA, <https://www.nena.org/?page=Standards>

²⁷ APCO International, APCO Project Retains, <https://www.apcointl.org/resources/staffing-and-retention/retains>.

- c. IT Support – determine how many people it will take to manage and mitigate (alarms, permissions, maintenance and any other necessary measures).
- d. Staffing needs will differ moving from legacy 9-1-1 to transitional 9-1-1 and then from transitional 9-1-1 to end step i3.
- e. Management knowledge of NG9-1-1, the deployment of NG9-1-1, etc.

4.10.2 Current Staffing Formulas, Profiles and Reports

Many of the existing staffing documents in use today were designed for legacy systems which have inherent limitations for how data is collected, sorted, stored and processed. Those documents may be a good starting point, but new staffing calculations for NG9-1-1 will need to be broader and use improved metrics to evaluate performance and the development of new standards. Without reliable data and improved tools, relying on outdated staffing models could negatively impact the success of the PSAP in the NG9-1-1 environment. Next generation technology won't do citizens or the public safety community any good unless the PSAP has the proper infrastructure and staffing in place to handle the influx of information that's coming.

WG2 believes that, at a minimum, PSAPs should comply with the NENA Call Answering Standard/Model Recommendation (56-005)²⁸ and should be staffed so as to comply with the 9-1-1 call answering standard identified within which states:

“Ninety percent (90%) of all 9-1-1 calls arriving at the Public Safety Answering Point (PSAP) shall be answered within ten (10) seconds during the busy hour (the hour each day with the greatest call volume, as defined in the NENA Master Glossary). Ninety-five (95%) of all 9-1-1 calls should be answered within twenty (20) seconds.”

There are other documents which make recommendations related to staffing, such as NFPA 1221,²⁹ NENA's Communications Center Staffing Workshop Tool, and APCO Project RETAINS report;³⁰ all provide some value but which many PSAPs find to be incomplete or cumbersome to use. Still other PSAPs utilize staffing formulas they've created based on personal experience and anecdotal information.

The TFOPA final report dated January 29, 2016 identified in Section 5.4, PSAP Optimization Options, cited four operational models for NG9-1-1 deployment.³¹ Each of the four types of implementations has both advantages and challenges as agencies begin to conduct discussions regarding the potential for physical optimization. Each of the models listed below need further consideration for staffing and training impacts in the NG9-1-1 environment.

1. Shared Services (Centralized)

A shared services center is where existing PSAPs are brought together under one roof or facility and share management and resources.

²⁸ NENA, <https://www.nena.org/?page=911CallAnswerStdnd>. The standard is currently under review and is expected to be updated in 1Q2017.

²⁹ National Fire Protection Association, <http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards?mode=code>

³⁰ APCO, <https://www.apcointl.org/resources/staffing-and-retention/retains.html>

³¹ FCC, Task Force on Optimal PSAP Architecture, Adopted Final Report, January 29, 2016, at https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf.

2. Hybrid

This model can include variations wherein PSAPs maintain separate physical locations but share common call handling, and other services such as radio, CAD or other public safety dispatching equipment over a secure managed network.

3. Centralized Call Taking Center

In this model, 9-1-1 calls, which would normally be directed to individual PSAPs, are routed to a centralized call taking facility.

4. Virtual

This mode requires shared infrastructure. The PSAP call handling equipment can be local or reside at a remote site or data center. An ESInet provides transport for the calls to be routed to the various PSAPs.

Regardless of which model a PSAP currently finds itself in or is moving towards, there are many critical factors to incorporate into a staffing study or when looking at appropriate metrics. The purpose of this report is not specifically to determine or list those factors, but to caution PSAP Managers and decision makers that work needs to be done on identifying staffing needs and new skill sets as legacy PSAPs transition into NG9-1-1.

Staffing requirements of the future could look very different. Many 9-1-1 telecommunicators have expressed concerns about NG9-1-1 and the amount of data, media, text and voice that will be flooding into their centers and impacts such volumes will have on responsiveness and staffing. Each center, depending on how they have optimized their operations, will need to justify their staffing requirements to policy makers and identify adequate and sustainable funding sources.

4.10.3 NG9-1-1 Staffing and Special Considerations

Special considerations will be necessary for PSAP Telecommunicator Hiring processes. New skill sets will be needed for 9-1-1 Telecommunicators. Some of those will include how broadband implications and implementations will affect the PSAP. APCO has initiated Project 43 (P43)³² that is examining a variety of issues related to broadband services, including NG9-1-1. As part of this initiative, staffing and personnel utilization are being studied. Other areas of study which will benefit PSAPs and public safety communications will also be included in the research and report. WG2 participants are hopeful that, when published, the P43 report and recommendations will result in additional resources, and guidance, for PSAPs that should be complimentary to the work done by TFOPA.

Public Safety broadband services, such as FirstNet, private and/or commercial networks, are leading to a paradigm shift in the role of the PSAP. Public Safety broadband services and NG9-1-1 can be complementary but are typically on separate planning and implementation paths. NG9-1-1 technology will enable PSAPs to utilize broadband data in ways that will transform how the public reaches 9-1-1 and how telecommunicators communicate with first responders. Other IP-based technologies, including those supported by smartphones, tablets, and mobile apps, are available throughout the general public and are capable of sending an array of information to the PSAP. As a result, PSAPs of the future will be the nerve center, managing data-rich communications via broadband technology with 9-1-1 callers and first

³² APCO, <http://psc.apcointl.org/2016/02/10/apco-launches-project-43-to-tackle-broadband-implications-for-the-psap>.

responders. 9-1-1 Authorities need to be mindful that NG9-1-1 and Public Safety broadband operations policies and procedures should be built into PSAP training and education.

PSAPs will need to consider what information goes directly to the PSAP and what information, if any, will bypass the PSAP and go directly to the first responders, investigators or relevant medical personnel. Operational impacts that require additional scrutiny include, but range well beyond the following:

- MMS Routing and Delivery
 - Where do the MMS requests get delivered?
 - How does that delivery occur?
 - How will the data be managed?
 - Who will be making decisions?
- HIPPA
 - Including what information may be provided, and to whom it may be provided.
- Telecommunicator skillsets: auditory, audio-visual and an abundance of data
 - How will Telecommunicators deal with the effects moving from an auditory environment to an audio-visual environment?
 - How will Telecommunicators handle dealing with the effects of an abundance of data, deciphering that data and pushing it out to the appropriate first responders?
- Telecommunicator Human Factors
 - Consider implementing specialized training
 - Consider implementing Employee Assistance Programs (EAPs)
 - Consider implementing Critical Incident Stress Management (CISM) Programs.

4.11 Lessons Learned: ESInet Early Adopter Case Studies

4.11.1 Introduction

WG2 was tasked with examining lessons learned in the implementation of Emergency Services IP-Networks (ESInets). The Working Group conducted a series of open-ended interviews to learn as much as possible from early ESInet builders moving towards NG9-1-1. The group began analyzing the data as soon as it was captured, looking for patterns between and among the experiences of a number of state, local and regional entities concerning the implementation of their own ESInets.

The interviews were conducted by WG2, using a set of benchmark questions. During this process, in-depth qualitative information was collected about their respective ESInet implementations. Flexibility in the interview process was utilized to optimize information gathering in the completion of this task. An example of this flexibility was multiple parties from the same agency being interviewed simultaneously.

The information has been organized into a table by major topic found in section 7.1. The purpose of this section is to provide an overview of that tabulation and to point out areas of commonality and differences between the interviews.

4.11.2 Early Adopter Case Study Participants

1. State of Maine Emergency Services Communications Bureau

The Emergency Services Communications Bureau is housed within the Public Utilities Commission. The statewide system has 26 PSAPs. The state took 18 months, once the contract was signed, to implement a total rebuild of the 9-1-1 system. They implemented PSAP CPE, ESInet, and core routing.

2. Iowa Department of Homeland Security and Emergency Management

There are 113 PSAPs in Iowa. Primarily this program is in charge of the wireless network. There is a little oversight on the wireline network, but mostly ensuring that local 9-1-1 service board plans are reasonable.

3. Commonwealth of Massachusetts, State 9-1-1 Department

The State 9-1-1 Department administers and coordinates the 9-1-1 system for 247 PSAPs in the Commonwealth of Massachusetts. The statute was revamped in 2008 to provide the authority to move forward with NG9-1-1. We also provide a disability access program out of this office.

4. Palm Beach County, Florida

Palm Beach County is the largest county east of the Mississippi at 2,000 square miles. The Office serves 18 PSAPs and about 150 positions. A secondary PSAP at Florida Atlantic University has also been established.

5. North Central Texas Council of Governments (NCTCOG)

NCTCOG is the 9-1-1 administrative entity serving 14 counties and 44 PSAPs surrounding the Dallas/Fort Worth area in North Central Texas.

6. Alta Vista Group, Boulder Regional Emergency Telephone Service Authority (BRETSA), Colorado

BRETSA is comprised of three primary PSAPs and one secondary on the CU campus. Boulder County has about 340,000 population and receives approximately 600,000 calls for service a year.

7. Indiana Statewide 9-1-1 Board

Indiana just completed a consolidation of PSAPs and now has 124 PSAPs across 92 counties. The board has handled wireless for a number of years while traditional wire line 9-1-1 has been handled on a local level. The state has recently been given the responsibility to expand their services to provide an equal level of service throughout the state.

8. State of Minnesota

The state program serves 99 primary PSAPs and 5 secondaries.

9. Verdugo Fire Communications Center in Glendale, CA

This newly created regional system exists with eight PSAPs today. The future plans are to have up to 22 PSAPs on the network in the future.

4.11.3 Case Study Details

4.11.3.1 Case Study Interview Categories

While the interviews were open-ended in order to obtain the greatest depth of qualitative data possible, a set of starter questions was used to ensure that a common core set of topic areas were covered.

1. *Overview.* An overview of the 9-1-1 program and the ESInet implementation project was obtained to provide a context for the rest of the interview. The ESInet implementations reviewed ranged greatly in project scope, from single, county-wide deployments to statewide deployments with multiple systems integrated into the new network. While this degree of variation offered the best chance at obtaining a well-rounded view of what could be experienced during an ESInet implementation, such variance can also account for differences in experience, and so such context is important. This overview included questions regarding how many Public Safety Answering Points (PSAPs) were to be encompassed in the network, whether the ESInet was truly “new” or built upon existing network architecture, and the timeline and duration of the implementation. Also asked was what the impetus was for the implementation.
2. *Planning.* Interview participants were asked to describe the 9-1-1 program, office, or entity that oversaw the planning of the ESInet, what kind of strategic plan was developed prior to implementation, and whether that plan changed throughout the process of implementation. Details were obtained about who the stakeholders were, the resources that were available and obtained for the implementation, and any implementation documents that were created throughout the process, such as Requests for Proposal, contracts, Scopes of Work, and others.
3. *Procurement.* The procurement process, as well as preparations leading up to the procurement process, were explored, starting with whether regulatory or statutory environments had to be adjusted prior to procurement. The funding of the project and establishment of costs were then discussed, followed by project scope, the vendor selection process, architecture, and what standards were used in the RFP, SOW, and SLA documents used in the procurement subsequent and implementation process.
4. *Implementation.* The questioning about implementation was more open-ended, with only some basic topic areas to start discussion, including technical issues faced by the PSAPs or because of technological variation at the PSAPs, training requirements for the PSAPs as well as for the vendor(s), challenges in working with the vendor(s), and any delays or changes to cutover timelines.
5. *Ongoing Operations.* Participants were asked how maintenance and support of the new network varied from their legacy systems, and whether new troubleshooting and support mechanisms had to be developed. They were also asked whether they experienced any major technical obstacles during the first few months of operation and how they resolved such technical issues. Similarly, they were also asked if there were any funding issues encountered during operation that were unanticipated such as unplanned costs. Questions about ongoing operations also considered the disposition of the legacy network, specifically whether there were or are components of the legacy network that had to be maintained and funded.

Finally, participants were also asked to name three things they felt went well with the implementation of the network, and any associated services, and three things they would do differently, as well as to “rate their implementation experience” on a scale of 1-10.

4.11.3.2 Case Study Interview Results Summary

This section summarizes the areas of commonality and variation discovered during the ESInet early adopter case study interviews. Full interview details can be found in Section 7.1-ESInet Early Adopter Case Study Interview Responses.

4.11.3.2.1 Planning

While the nature of this type of inquiry creates narrative responses that are difficult to compare on a point by point basis, some patterns do emerge. For instance, in questioning participants regarding *planning*, planning activities varied in duration from about a year or less (ex: NCTCOG, Indiana) to several years prior to implementation (ex: Massachusetts, Palm Beach). Nevertheless, this wide variation reveals that the interview participants all went through extensive planning processes that seem to fit into two categories: long and deliberative or short and focused, and that whether the implementation fell into one category or another didn’t seem to be overtly related the size of the implementation being considered.

Some of the variation in the duration of the planning process may be due, in part, to what the motivation was for implementation. BRETSA’s pursuit of an ESInet was necessitated by a change in Computer Aided Dispatch (CAD) vendors that required an ESInet to connect the PSAPs within the county-wide 9-1-1 Authority, for example, which created a sense of urgency that likely compressed the planning process. The Commonwealth of Massachusetts, on the other hand, implemented their ESInet after over seven years of planning, and could take such time since there wasn’t a pressing need to implement sooner.

The resources used to implement the ESInet, from planning to execution, also varied widely. The state of Iowa, for instance, used almost all outside contracted resources, having only two FTEs to work with internally, an approach similar to the one utilized by the State of Indiana. An opposite approach was taken by the Commonwealth of Massachusetts and the North Central Texas Council of Governments (NCTCOG), both of which increased their internal workforces to handle the IT, GIS, and administrative demands in-house. This variation might be a reflection of the governance structure that existed and whether the expansion of workforce within that structure was an option, and it might also reflect the vendor relationship chosen for implementation. In a vendor relationship where ESInet implementation and operation is being purchased as a service from the vendor, for instance, a smaller workforce might be necessary, while a network being run by the ESInet governing body would necessitate a larger pool of internal resources. More interestingly, however, is the fact that like the duration of the planning phase, most of the ESInet implementations seemed to fall into one of two categories. With the duration, it was a dichotomy between compressed/focused and long/deliberative planning processes, while concerning the issue of resources the dichotomy is between a model of core internal resources and “outsourcing” to the vendors of technical skill on the one hand and a significant expansion of internal resources and more direct management of vendors on the other.

All of the participants reported the creation of a large array of documentation and artifacts and have memorialized these documents for historical review.

4.11.3.2.2 *Funding and Costs*

There was little commonality in the area of funding, which may not be surprising due to the variation in funding models in place for legacy 9-1-1 system operations among the states and local entities that were interviewed. Some of the programs, including BRETSA and NCTCOG, funded their implementation primarily through existing 9-1-1 funding sources. Most of the programs, however, changed or increased their funding mechanisms to support implementation and operations. The State of Maine took a unique approach of temporarily increasing surcharge funding to support implementation by using cost savings through their operational strategy to reduce funding following implementation. Palm Beach was able to obtain several million dollars in grant funding from the state, highlighting what may be a difference in funding opportunities between local and state-level implementations. In all cases, recognition was given to “start-up” cost requirements and ongoing operational funding requirements.

Costs also vary, reflecting strongly the scope and implementation strategy. Where the 9-1-1 program overseeing the implementation owns and operates the network, upfront costs are necessarily more pronounced. BRETSA, for example, estimated initial one-time costs of \$400,000 for fiber and components, which is not insignificant for a one-county ESInet. The State of Minnesota, similarly, estimated starting costs of close to \$9 million.

Another major factor in the cost of the ESInet depended on the scope of what the ESInet was intended to accomplish. In BRETSA’s case, for instance, the ESInet was intended primarily to carry data for their CAD system, not as a transport for a Next Generation 9-1-1 network. Iowa, on the other hand, intended their ESInet be transport for an i3-compliant NG9-1-1 network with enough bandwidth to handle photos and videos when the time to implement such features arrives. Building a network for CAD data versus building a network for voice and multimedia traffic will necessarily result in different cost structures.

4.11.3.2.3 *Implementation*

The duration of the actual implementation phase varied widely based on the scope and implementation strategy, although it’s difficult to point to a particular factor that may underpin those differences. NCTCOG had an external time frame imposition requiring the implementation of forty-four (44) sites in only six months. On the other hand, the Commonwealth of Massachusetts has prioritized testing over the speed of implementation, and is still early in the implementation phase after over a year in the testing phase. Implementation durations may be more of a function of external constraints on time frames and comfort with testing regimes than of architecture or governance structures.

Several of the participants reported technical issues, with two of them - the State of Maine and Palm Beach - reporting audio quality issues, while NCTCOG notes that the arrangement of a network into a host/remote architecture means that outages tend to affect larger areas.

Training of Telecommunicators has been integrated into the implementation process by all of the participants, with one recurring theme being the timeliness of training and the difficulty in ensuring that training was received in a close enough time-frame with an implementation that the benefits of training were not lost before the actual implementation. This also translated into additional costs, with California noting the need for overtime pay to cover training costs and Minnesota contracting with community colleges to build online training tools.

4.11.3.3 Ongoing Operations

A majority of the participants noted improvement, and in some cases initiation of, processes in notification, monitoring, trouble tracking, and change management. Based on the participants' comments, this increase in situational awareness and follow-through on trouble tickets may be one of the unexpected benefits of ESInet implementation, as all of the participants seem to have taken advantage of the monitoring capabilities of IP-based networks to improve their processes. This may even reach a point of diminishing returns, as the State of Minnesota noted that they receive too many network event notifications over conditions that don't affect the operation of the network, which may indicate that consideration of what thresholds should necessitate notification of the governing body may need to be a planning component.

One participant noted a concern with unforeseen expenses. The State of Minnesota noted that they are paying Universal Service Fund fees on their IP networks, which they didn't anticipate being charged by the vendor and didn't include in their original cost estimates. It would be useful to return to the other interview participants to see if any of them are also paying these fees and if they anticipated paying these fees prior to implementation.

4.11.4 Conclusions

This short summary of conclusions drawn is not intended to be a complete enumeration of all of the comparisons, contrasts, and highlights to be found among the interviews of the ESInet implementation participants, but rather to provide some examples of the types of insights which might be gleaned from them. A table of ESInet early adopter interview responses can be found in Section 7.1 and may be useful for further comparison. Based on the discussion above, the following conclusions were drawn:

4.11.4.1 Planning

It is vital to have a strategic plan. The duration of the planning process is strongly influenced by the project scope and implementation timeframe. The interviews identified some that had an immediate need for connectivity only (as a first phase), as well as those that were working to build an IP transport which is foundational for their NG9-1-1 i3 system. An early decision to be made in the implementation process is whether to manage the ESInet in-house (owned and operated model), potentially requiring a build-up of in-house resources, or to allow a vendor to manage the ESInet (managed services model). It is important to evaluate the environment and identify operational, support and related skills of 9-1-1 stakeholders through site visits. Documentation of the process needs to be thorough at every step, including planning, vendor selection, design, testing, implementation, monitoring and ongoing maintenance.

4.11.4.2 Procurement

The scope and size of the project have the greatest impact on costs. Many of the interviewees stated the importance of including contingency planning in the form of diversity of paths, transport methods (e.g. fiber, microwave, wireless, etc.) and vendors. Some respondents included potential plan expansion to include future multi-media and broadband. Most of the interviewees intended to build a standards-based Next Generation system, but many admitted there are challenges in that many standards are dynamic and it is difficult to predict changes. Existing funding mechanisms may be sufficient, depending on the scope of the project, but practitioners should be prepared to be creative when it comes to sustainable funding.

4.11.4.3 Implementation

The duration of the implementation phase will vary based on scope, internal and external time constraints, resources, and the comfort level the 9-1-1 Authority has with the speed of the implementation and testing. Vendor changes (i.e., acquisitions, mergers) mid-contract can also impact the implementation timeline

and should be addressed in the “Terms and Conditions” of contracts. Collaboration and effective, regular communication is a cornerstone of implementation progress. Most implementations are not without technical challenges. Planning for dealing with these during implementation and planning reasonable time for testing and resolution of problems may create a more realistic timetable. Issues can be resolved globally only if they are effectively communicated. Effective training, starting with understanding the scope of operations and changes to work processes, is a cornerstone of operational continuity. Training timetables need to be flexible to accommodate changes in implementation timeframes.

4.11.4.4 Ongoing Operations

9-1-1 Authorities should take full advantage of the system’s operational monitoring and situational awareness capabilities. In addition to vendor monitoring, 9-1-1 Authority self-monitoring through staff and software, managed service contracts for monitoring or a combination of both were used by all of the interviewees. Network Operations Centers become more important than in the legacy world for monitoring, notification, and management of outages. Maintenance models change with NG9-1-1. Preventative maintenance, reporting and trouble ticket systems, resolution (more can be handled remotely, but does not replace the need for periodic onsite support), and troubleshooting processes need to be part of Next Generation planning. GIS changes from a “nice to have” to a “must have” and there is a great deal of GIS work that needs to be completed and maintained to have a successful NG9-1-1 system. This will result in a need for additional specialized GIS resources (in-house or contracted) for rectifying map borders, comparing MSAG to GIS to improve map accuracy and geospatial routing. Forward looking GIS maintenance support resource requirements and process discussion is an important part of ongoing services continuity.

The common thread throughout the interviews was the respondent’s willingness to share their experiences. The early adopters gave of their time for this interview and each of them agreed to field additional questions from others in the future. The writers encourage everyone in the planning stage for NG9-1-1 implementation, add research to your plan and reach out to the early adopters.

5 Recommendations

The following recommendations are delivered to those responsible for the implementation and delivery of NG9-1-1:

1. Establish a formal governance structure, consistent with statutory requirements, if applicable, for the purpose of collaborative planning, implementing and operating, which may necessitate outreach to currently non-participating entities.
2. Develop a strategic NG9-1-1 transition plan
3. Begin GIS dataset development and/or enhancement early as the magnitude of this activity is sometimes underestimated. GIS data format, collection, and maintenance in the design of the system and systems operations must be considered. This effort may need to be included as part of your Governance planning and must be in concert with the Forrest Guide. It should meet existing or developing standards for mapping interoperability.
4. Be diligent in the development of the Request for Proposal (RFP), and be specific as possible when addressing system requirements. For example, not just requiring the installation of anti-virus protection for all hosts, but also specifying the policy and procedures associated with it (e.g., the frequency at which it should run).
5. Plan for the delivery of NG Core Services as an integral component of the NG9-1-1 transition plan
6. Consider cybersecurity in the design of the system and system operations. Security guidance is available, including National Emergency Number Association (NENA) standards (specifically the i3 and NG-SEC standards), INFOSEC standards, and other security standards. Best practices from NIST, ISO, COBIT and others can also be used to inform security operation.
7. Identity, credential, and access management (ICAM) solutions must be considered to ensure identity proofing and data integrity in order to create a framework for user registration, verification, authentication, and authorization. The ICAM structure is integral to the NENA i3 Architecture design. As solutions are evolving, stakeholders should remain cognizant of the developing standards.
8. Ensure traffic engineering studies and mapping of service areas are current and incorporated into system design.
9. Evaluate all aspects of staffing related to NG9-1-1 planning, implementation and operations, on-going and future. The evaluation should include the roles of all stakeholders at all levels.
10. Observe existing systems and engage with owners/operators of systems under consideration before choosing a vendor or even writing an RFP.

11. Engage in comprehensive testing of new system software and hardware before transitioning to live operations to ensure all attributes and services are implemented correctly and meet expectations.
12. Review standards and available services with a local mission perspective, choosing to adopt only attributes/services that will benefit the unique circumstances of the area served.
13. Maintain positive relationships with contributing entities (e.g., call taking staff, local database administrators, vendors, service providers).
14. Remain engaged in enforcement of system expectations, and vigilant for issues.
15. Allow for modification after implementation, understanding that some features may need to be turned off or revised after implementation.
16. Have a planned approach to NG9-1-1 adoption and remain in control of the pace of system evolution.
17. Identify technical staff whether internal, third party or a combination, necessary to manage this very sophisticated technology.
18. Prepare for operational changes in the PSAP to address on-going issues in areas like CAD, GIS accuracy, IT, training and staffing, data management and other new technologies.
19. Convene a multidisciplinary stakeholder Advisory Committee, at a national level, to focus on NG9-1-1 issues. The goal of such a committee would be to promote the effective integration of technologies, resources and processes related to the development of the NG9-1-1 National End State.
20. Recognizing the enormous and fragmented scope of this effort, Congress should take action to ensure that the development of a NG9-1-1 End State across the country is adequately funded, staffed and coordinated.
21. Recognizing the critical importance of cybersecurity and associated required training, it is the recommendation of the Working Group that cybersecurity training guidelines are created and implemented.

6 Conclusions

The development and implementation of NG9-1-1 has been progressing slowly across the nation for all the reasons previously discussed in the TFOPA Final Report as well as this Supplemental Report. What has been clear during this transition is that there has been an ongoing cloud of confusion and misunderstanding with many in the 9-1-1 community, as well as the public, as to what exactly this new paradigm of 9-1-1 will entail.

Although much outstanding work has been accomplished conceptually and in the development of various technical standards, the understanding among the 9-1-1 Authorities that will need to plan, design, implement and operate these Next Generation technologies has been limited. This is through no fault of their own. It is difficult to fly an airplane while it is still being built so to speak.

What has resulted is in many circumstances is a misconception of what exactly NG9-1-1 is and a misunderstanding of what the ‘end state’ must be so as to know when a 9-1-1 Authority has implemented a fully matured NG9-1-1 system. Many saw this evolution occurring solely within the Public Safety Answering Point (PSAP) which has been the focal point for 9-1-1 over the past 40 plus years. Clearly not fully understood was the depth and detail of the transition from TDM to IP and the new component pieces that would create a new way of doing business with dramatically transformed changes in the NG technology platform.

In TFOPA’s Final Report Section 5, WG2 spoke to the general requirements that 9-1-1 Authorities would need to consider as they braved this new world and reached out to develop new relationships and new partnerships. Stepping outside of the current walls and controls of an individual PSAP can be a frightening leap of faith for some. But it is clear that the paradigm has shifted and the evolution of a new way of technically providing 9-1-1 services is upon us. Existing 9-1-1 Authorities must reach out to neighbors and seek new ways to join forces to provide a more robust and comprehensive organization. NG9-1-1 technologies will be shared across current boundaries. In some areas of the nation this is already occurring with “early adopters”, but in many areas it has unfortunately not even begun. 9-1-1 Authorities and elected officials at all levels of government have a duty and obligation to their service area citizens to begin actively moving forward to advance NG9-1-1 in their communities.

WG2’s goal in this Supplement to the TFOPA Final Report has been to more specifically identify the elements and actions required to transition to full NG9-1-1. The Supplemental Report is intended to assist PSAPs, 9-1-1 Authorities, government interests, policy development groups and all parties by providing a straightforward checklist which can then be used for planning and implementation as 9-1-1 Authorities move through the NG9-1-1 maturity states.

The “NG9-1-1 Readiness Scorecard” developed through this process is designed to provide clear guidance to the 9-1-1 Authorities of the road before them and act as a map for planning. Although we clearly understand this will not be easy, it is essential to understand the necessary elements involved in the NG9-1-1 transition. As we have previously said, this process is not necessarily linear. Elements associated with a particular implementation state can, in some cases, be implemented in parallel with elements of another state. For example, an ESInet can be implemented while the GIS dataset is being created. Ultimately however, both need to be completed and in place in order for geo-spatial routing of 9-1-1 service requests to take place.

A true nationwide NG9-1-1 system needs to be developed and implemented. Building and implementing a NG9-1-1 End State is not merely a local, regional, or state challenge; however, during NG9-1-1

transition, regions will be reaching across their boundaries to interoperate with neighboring regions. Additionally, States must also interoperate with other states.

Although this Supplemental Report can be read and used as a stand-alone report, we encourage readers to also review the TFOPA Final Report approved January 29, 2016. These two documents together will serve elected officials, 9-1-1 Managers, and 9-1-1 Authorities to better understand the challenges they have ahead of them through the evolution of steps to NG9-1-1 End State.

The need to move to multi-media NG9-1-1 is essential. The citizens desire it, the deaf and hard of hearing community requires it, and the 40 plus year old TDM switched environment has reached end of life. We can move forward now in a planned transition or we can wait, deny, or resist and ultimately reach a point of crisis in 9-1-1. There is no doubt what the prudent and responsible choice should be regardless of difficulty and challenges.

7 Appendices

7.1 ESInet Early Adopter Case Study Interview Responses

This section contains the actual responses provided by the stakeholders during the case study interviews. The following represents both ESInet and NG9-1-1 early adopter case studies. This will include not only ESInet implementations but also various other elements required within the NG9-1-1 Implementation Continuum described in this report.

TOPIC	EARLY ADOPTER RESPONSES
Planning	
<i>Planning</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> Grew staff in anticipation of the NG implementation. The state took contract GIS resources and added them to the 9-1-1 staff as full-time employees. Job descriptions, policies, and procedures were updated. Identified new places for people to develop. GIS was the biggest area of change. GIS used to be a “nice to have” and now it is the basis for the whole system - the critical path. <p>State of Iowa:</p> <ul style="list-style-type: none"> Had existing infrastructure in the form of a fiber network called the Iowa Communications Network. Able to add all the PSAPs to the network, which carries the wireless traffic. Some VoIP calls traverse the network as well. <p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> Has planned NG9-1-1 implementation for over seven years with vendor presentations, attendance at industry conferences, development of an RFI and RFP, as well as hiring a consultant. ESInet is dedicated to 9-1-1. There will be two carriers into each PSAP. Currently utilizing cloud based computing and the WAN. Investigated and tested satellite for some of our larger PSAPs. <p>Palm Beach County, FL:</p> <ul style="list-style-type: none"> Started as an early adopter with an RFP in 2009 and initial implementation in 2011. System includes two data centers, one in Orlando in a vendor Central Office and one in an Orange County government data center. Contract will be ending soon and the county is considering the best route for moving forward. When this project started, no one had done this so it was all about best effort. A great deal has been learned in the past five years. <p>NCTCOG:</p> <ul style="list-style-type: none"> NCTCOG began planning in 2007 and implemented the first ESInet and IP CPE in a six month period in 2008. The next two years were focused on stabilizing the new system, then adding 2 geographically diverse data centers (outside of the PSAP environment), core services, a virtual environment and text to 9-1-1. Currently working on adding different mediums to the network with a microwave overlay and business class internet to supplement the current MPLS

TOPIC	EARLY ADOPTER RESPONSES
	<p>fiber and LTE wireless backup. All of these projects have been part of a plan that is dynamic and flexible and has grown with the program.</p> <p>BRETSA:</p> <ul style="list-style-type: none"> Went with a phased approach due to funding limitations and lack of commercial availability. Planning became a necessity when the CAD vendor provided prerequisites that could not be met without making some upgrades to redundancy and GIS. Unique in that one CAD server among four PSAPs. So while Next Generation 9-1-1 was not the original purpose, it has become an accomplishment. <p>State of Indiana:</p> <ul style="list-style-type: none"> Spent six months evaluating the 9-1-1 system in 2013 and decided to implement an ESInet for wireless. There was an existing wireless network for call delivery in a percentage of the state and that would be upgraded or enhanced to transition to Next Generation 9-1-1. The board decided in the best interest of public safety, to provide the opportunity to have more than one vendor operate more than one ESInet across the state. The RFP process took another fourteen months. <p>State of Minnesota:</p> <ul style="list-style-type: none"> Utilized consultants for a trend assessment and report in 2008 and then went into procurement. Developed a State 9-1-1 Advisory Committee and chose to implement classic standards based ESInet using T-1s, with Legacy PSAP Gateways on one side and Legacy Selective Router Gateways on the other side. We provide the transport in the middle. We followed a phased approach and it took a little over two years to get all of our PSAPs connected. There were challenges with the state radio program competing with 9-1-1 for funding. The solution was to incorporate NG9-1-1 into the radio governing board (the statewide emergency communications board) and now they review all requests and are able to better allocate resources and funding fairly. <p>CA Ring:</p> <ul style="list-style-type: none"> Research began in 2008, got state approval for a pilot in 2012 and began procurement and implementation of eight PSAPs with new hosted and managed CPE and IP connectivity in 2015. The next phase will be to add Voice to the IP network. The group has identified an additional 14 PSAPs that could realistically join the network in the future. However, the case has been proven with the current eight.
<i>Resources</i>	<p>State of Iowa:</p> <ul style="list-style-type: none"> With only two FTE's, relied on the additional resources of a consulting firm and contractors. <p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> Had to infuse more IT knowledge and project management into the staff in order to be positioned for the transition. It is great to have in-house expertise as a double check for what the vendors promise and to make sure it is delivered. <p>Palm Beach County:</p> <ul style="list-style-type: none"> The county has built an IT team and developed a strong relationship with the County IT department and vendors.

TOPIC	EARLY ADOPTER RESPONSES
	<ul style="list-style-type: none"> • Staff no longer sits back and waits for things to be fixed. The county purchased tools and invested in monitoring and troubleshooting. The county partners with vendors and helps them with problem identification and remediation. Relationships are key and mutual trust has been established. • Hired a full-time project manager to manage deployments. <p>NCTCOG: There were problems with service that led to a business case justification to take maintenance in-house. This meant beefing up GIS staff and creating a technology team for installation and maintenance. They are dedicated to 9-1-1 with specializations in legacy, IT, and network.</p> <ul style="list-style-type: none"> • Also used consultants to lead the procurement, assist with project management, provide staff training and supplement subject matter expertise. <p>BRETSA:</p> <ul style="list-style-type: none"> • Developed a CAD core team made up of the four PSAP managers, project manager/consultant and four tech team representatives (one from each of the PSAP's). The core team meets weekly to make decisions and assign work for the coming week. <p>State of Indiana:</p> <ul style="list-style-type: none"> • Hired consultants because staff is small. Did not have in-house staff for technology, legal or procurement. Consultants created the RFP and SLAs and the Indiana Department of Administration assigned us procurement officials free of charge. Legal was sourced out and the state continued a professional services contract with consultants for an expanded scope of work. <p>State of Minnesota:</p> <ul style="list-style-type: none"> • Hired consultants for professional and technical services in addition to staff. <p>CA Ring:</p> <ul style="list-style-type: none"> • Gathered major stakeholders (Police and Fire Chiefs, City Managers and IT) and took them to the Rose Bowl for a presentation and demonstration by vendors, SMEs and staff. Achieved buy in and they have supported the project ever since.
<i>Artifacts</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> • A well-written RFP is critical. That document is what vendors use to develop their plans. It will also be the template for a testing plan. The state utilized a consultant and an attorney to write the RFP. <p>State of Iowa:</p> <ul style="list-style-type: none"> • A consultant conducted a feasibility study and developed a checklist and strategic plan that staff tries to keep up to date. They also developed the PSAP specifications. <p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> • Developed a great RFP document. It is based on NENA standards and is very specific about the components and relevant standards. <p>Palm Beach County:</p>

TOPIC	EARLY ADOPTER RESPONSES
	<ul style="list-style-type: none"> Keep all documents on a SharePoint site. Everything associated with the project is on that site and organized in folders to make them easily searchable. It is important to document everything in order to learn from history. Also have very detailed network management drawings of infrastructure to help with trouble resolution. <p>BRETSA:</p> <ul style="list-style-type: none"> Used a cloud solution for document management. Dropbox was used with access granted to all involved. The project plans, timelines, checklists and lessons learned are all stored there. <p>State of Indiana:</p> <ul style="list-style-type: none"> All SLAs, contracts and other documents that have been redacted to remove proprietary information or stored. All of the documents are in a single packet to be provided upon request. The goal is to make those available in individual documents on a website in the future. <p>State of Minnesota:</p> <ul style="list-style-type: none"> Archived all relevant documents (Test plans, MOPS, problem scenarios, etc.) into a cloud server and then made thumb drives for all. Talking about putting some on the website and are willing to share.
Procurement	
<i>Leg/Reg</i>	<p>NCTCOG:</p> <ul style="list-style-type: none"> The regulatory issue faced was a PUC requirement to be a certified telecommunications provider in order to selectively route 9-1-1 calls or host a 9-1-1 database. This forced a hybrid solution. NCTCOG has since gained the certifications. <p>State of Indiana:</p> <ul style="list-style-type: none"> A legislative change gave the state responsibility for wire lines as well as wireless, creating a statewide 9-1-1 authority responsible for all 9-1-1 delivery in the state.
<i>Funding</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> Estimated the cost for the new system as well as the costs of running two systems at once during the implementation. Went to the legislature and asked for a 5 cents surcharge increase to cover the 18 month implementation period. The bargaining chip was the promise to reduce the surcharge 10 cents following implementation, the 5 cent increase plus an additional 5 cents, showing the efficiency of the changes. The legislature and governor liked the idea so much that they funded the additional costs for implementation through a general fund appropriation instead of raising the fee. In addition, when it came time to lower the rate as promised, the legislature made the decision to keep the current rate. <p>State of Iowa:</p> <ul style="list-style-type: none"> The state has a dual network model (wireline and wireless) and also a dual funding model. The wireless fees were set at 63 cents but the local service boards set their own fee per county at anywhere up to one dollar. The state standardized the fee to one dollar across the board, with part of the local service board funds going to pay for the network.

TOPIC	EARLY ADOPTER RESPONSES
	<p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> Collected a surcharge of 75 cents for seven years and then got it increased to \$1.25 for a year and now it is at \$1. That fund is going to pay for the entire implementation according to the contract and cost projections for the next five years. <p>Palm Beach County:</p> <ul style="list-style-type: none"> In 2008, received a 6.5 million dollar grant from the state and the county had over 4 million dollars to add to that for the Next Generation 9-1-1 transition. <p>NCTCOG:</p> <ul style="list-style-type: none"> Legislative funding limited the ability to partner with others and conduct long-term planning. NCTCOG is funded through the legislative process on a two-year cycle. The appropriations are based on the state of the Texas economy and achieving a balanced budget. <p>BRETSA:</p> <ul style="list-style-type: none"> Have been successful using 75 cent surcharge to fund the 9-1-1 transition, Pictometry, lobbying, DropBox, and a fiber network. Because money is collected locally, there is no risk of state diversion or raiding of funds. <p>State of Indiana:</p> <ul style="list-style-type: none"> Needed an increase in the fee that required legislative action. Formed a coalition of stakeholders and together were a strong enough voice to get the fee raised. <p>State of Minnesota:</p> <ul style="list-style-type: none"> Utilized E9-1-1 funds exclusively for the ESInet deployment. The state also got an NTSA grant for up to \$10,000 per PSAP for PSAP equipment rooms.
<i>Costs</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> The state has seen cost savings from the Next Generation implementation. The costs for a typical 4 position PSAP went down from \$12,000 a month to \$2,000 a month. The savings are about \$10,000 a month per PSAP. <p>State of Iowa:</p> <ul style="list-style-type: none"> The non-recurring cost to buy equipment for the 2 data centers and all of the equipment to connect the PSAPs to the network and training was around \$4 million. Recurring costs for the network and management is around \$2 million per year. <p>Palm Beach County:</p> <ul style="list-style-type: none"> The county tracks expenses and funding very carefully. They know the cost per call and per position, and break down expenses for circuits, software, and maintenance. <p>NCTCOG:</p> <ul style="list-style-type: none"> Had an initial budget of 6 million dollars in 2008, which included consulting fees, new IP, CPE and ESInet.

TOPIC	EARLY ADOPTER RESPONSES
	<p>BRETSA:</p> <ul style="list-style-type: none"> Estimated about \$400,000 on one-time costs for fiber, Internet, switches, firewalls, security, monitoring, and encryption. Continue to pay about \$120,000 annually in recurring costs. <p>State of Minnesota:</p> <ul style="list-style-type: none"> The initial project cost was about 9 million dollars, with the ongoing monthly cost of just over \$500,000. <p>CA Ring:</p> <ul style="list-style-type: none"> All funding comes from the California state 9-1-1 office. There were some challenges with their CALNET contract for purchasing. CALNET 1 only allowed for CPE. They solved the problem with CALNET 2, which allows for network cost.
<i>Scope</i>	<p>State of Iowa:</p> <ul style="list-style-type: none"> This system is an end to end solution based on NENA i3 standards. The state built enough bandwidth capacity to support photos and video down the line. They are also keeping an eye on the FirstNet project in the state to identify any potential synergy. <p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> Made sure to include physical diversity in the RFP. Also identified PSAPS to act as pilots to find lessons learned for the rest of the deployment. Technical requirements held the greatest weight in the evaluation of responses, but the cost was considered as well. There is supplier diversity in Massachusetts and a prompt pay discount. <p>Palm Beach County:</p> <ul style="list-style-type: none"> Deploying LTE wireless mode for backup for a number of PSAPs, especially those on the Barrier Islands. The county has mobile PSAPs in which they are exploring LTE. Sharing or collaborating in the future with FirstNet based on the potential is a long term goal. <p>BRETSA:</p> <ul style="list-style-type: none"> While the scope was primarily for CAD, they learned connectivity and interoperable solutions in the PSAP were a necessity. Used MOUs and agreements to build a regional 9-1-1 solution. <p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> The scope has changed over time, mainly moving from government providers without SLAs to more private sector solutions to improve service level agreements. Cheaper is not always better when dealing with mission critical systems. The Commonwealth has worked on redundancy and diversity in the network and has seen challenges with the construction of the last mile. <p>State of Minnesota:</p> <ul style="list-style-type: none"> Used a phased approach. Phase I was designed to provide connectivity/interoperability for all PSAPs in the state. This was a huge step to allow for call transfers with ANI/ALI between all PSAPs. 40,000 successful

TOPIC	EARLY ADOPTER RESPONSES
	<p>transfers in the first year demonstrated the success. Phases II and III were designed for voice migration.</p> <p>CA Ring:</p> <ul style="list-style-type: none"> From a continuity of operation standpoint, it was important to have the ability to log in from anywhere on the new network to take calls until another PSAP could relocate to a backup in a disaster situation.
<i>Vendors</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> The State of Maine procured one contractor (prime) with sub-contractors. Once a month they get a single bill, broken down into components. It was not an easy process. There were 9 quality bids, but there were two appeals, which delayed the process an entire year. <p>State of Indiana:</p> <ul style="list-style-type: none"> Utilized a menu selection in procurement. It was not one vendor take all. Multiple ESInets across the state provides redundancy and an equal level of service. The approach also allowed cost savings on enhanced services. Encouraged the vendors to describe how they would meet state objectives, instead of tying them to a solution developed by Indiana. <p>State of Minnesota:</p> <ul style="list-style-type: none"> There were only two responders to Phase I for the connectivity and both were awarded to get the interoperability desired. There was only one award for Phases 2 and 3. <p>CA Ring:</p> <ul style="list-style-type: none"> This system used a managed service relationship with a vendor and it has been successful. However, they were challenged a couple times by vendors who were sold to another company in the middle of the project. This causes time delays, change in project management philosophy and personnel.
<i>Architecture</i>	<p>State of Iowa:</p> <ul style="list-style-type: none"> The state is in the process of building a secondary ESInet that is completely redundant using a different vendor for diversity. The network will only serve the 13 largest PSAPs in the state and is designed for outage management (planned or not). The 13 PSAPs would be able to handle all of the state's 9-1-1 traffic using different ingress into the PSAPs and different fiber from a different provider. <p>NCTCOG:</p> <ul style="list-style-type: none"> Leased commercial MPLS because it was readily available in the area and very economical. With the creation of a technology team, NCTCOG duplicated some services to get the best service possible. NCTCOG got monitoring software and also contracted for monitoring services. The NCTCOG technical team assisted with implementation to learn the system, but paid the vendor to be the primary installers. These were duplications that really paid off.

TOPIC	EARLY ADOPTER RESPONSES
	<ul style="list-style-type: none"> There is still a contract for tier 2 or backup maintenance, in the case of a disaster. With 44 PSAPs, one cannot afford to build a team large enough to handle a disaster. <p>BRETSA:</p> <ul style="list-style-type: none"> BRETSA has a hybrid architecture. The primary site is in Boulder and the backup is in Longmont, which provides geodiversity and different terrain. They are going from a more traditional client-server WAN, to include more hyper-convergence, and virtualization to save costs on configuration and support. <p>CA Ring:</p> <ul style="list-style-type: none"> There are two geographically diverse NCCs – one in Pasadena and one in Ventura County, with an aggregation point in Hollywood, all in a ring configuration.
<i>Standards</i>	<p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> RFP is full of specific NENA standards, including a great deal of depth into security. <p>Palm Beach County:</p> <ul style="list-style-type: none"> The NENA standards were in the RFP, but they are still evolving. A trust factor was needed with the vendors to follow the standards as they evolve. <p>NCTCOG:</p> <ul style="list-style-type: none"> With standards constantly evolving, the RFP stated: “will meet the current NENA standards”. It was generic, but the vendors understood the desire for a standards based system for interoperability and growth. <p>BRETSA:</p> <ul style="list-style-type: none"> Standards were included from NENA and others. The CAD core team makes the standards decisions based on their experiences reported through the weekly meetings. <p>State of Indiana:</p> <ul style="list-style-type: none"> Suggested a design based on the NENA i3 standard. <p>State of Minnesota:</p> <ul style="list-style-type: none"> Tried to build a standards based solution. One of the challenges has been that many standards are not finalized, so it is unknown what will happen next.
Implementation	
<i>Implementation</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> 18-month deployment – not a flash cut. Started with one PSAP at a time but eventually were cutting two PSAPs a week. There is a time when one should run two systems, and there were various steps occurring at the same time throughout the 18 months. Don’t overlook the importance of testing. Lab testing is good, but there are some scenarios that can’t be tested in a lab and that means a good test plan is needed for the field.

TOPIC	EARLY ADOPTER RESPONSES
	<ul style="list-style-type: none"> One of the lessons learned during testing was regarding backups. At one point, all the calls were going into a loop and the state had to revert back to the old system. It delayed the project a month, but the problem was resolved and the dual systems really paid off. PSAPs didn't lose any calls, and it was the right thing to do. <p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> Testing has been a priority. The Commonwealth tested for over a year in the lab and in a pre-integration environment. They test at 200% capacity. The Commonwealth thought they would have been further along than this, but are being very cautious. The pilot PSAPs are all unique and testing failure scenarios have revealed issues that have been resolved before full implementation. They kept the old gear in place so it could be rolled back if necessary. <p>NCTCOG:</p> <ul style="list-style-type: none"> The most challenging part of the implementation was the schedule. With 6 months to implement 44 sites, it was tight. When a problem is identified, everything has to stop until it is corrected. When it takes time, the implementation and training schedules must be revised. <p>BRETSA:</p> <ul style="list-style-type: none"> Created an ops team to assist with implementation. Each ops team member acts as a system administrator and lead. They have different skills sets so there are SMEs in the system. BRETSA pays for their time when they are planning for the system. It is a good concept that has been a win/win for the PSAP and BRETSA. <p>State of Minnesota:</p> <ul style="list-style-type: none"> Used the same team for installation of the equipment throughout the state for consistency and still have them on contract for equipment maintenance. <p>CA Ring:</p> <ul style="list-style-type: none"> It is extremely important to have the vendors come in with an assessment team to evaluate the PSAP environment and find gaps that need to be addressed.
<i>Technical</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> A problem that used to affect a PSAP now affects all of them, or at least half of them. There were some audio issues across the board that required work with the voice quality of the calls. There were also a lot of decisions to be made with the software and settings in the beginning. Some of those changes needed to be standardized throughout the system and some were customizable at the PSAP level. A checklist for each PSAP was developed to make sure all the potential changes were addressed. <p>Palm Beach County:</p> <ul style="list-style-type: none"> There were big problems with echo issues. Troubleshooting revealed that the pitch of the voice or a background noise could trigger an echo. The monitoring software isolated the problem to the firmware.

TOPIC	EARLY ADOPTER RESPONSES
	<ul style="list-style-type: none"> • There were also problems with the ESInet collapsing. All calls would drop randomly, so the county worked with the vendors to set up a lab and found the problem in the core router with a software glitch. • The county has been very involved in isolating and troubleshooting problems across the board. They worked with a vendor to set up a dashboard to watch call volume real time. <p>NCTCOG:</p> <ul style="list-style-type: none"> • Being part of a host/remote system brought some technical issues, mainly that now 11 – 44 PSAPs went down with an outage instead of one. NCTCOG divided their regional system into four hosts and four redundant backups that eventually became active/active, which solved our multiple outage problems. • They had network challenges with outages and fiber cuts as well. It was a challenge dealing with fiber providers that didn't understand there is no maintenance window in 9-1-1. <p>State of Minnesota:</p> <ul style="list-style-type: none"> • The PSAPs were challenged by space needs. The state used the same two people to go to each PSAP for site surveys/readiness evaluations for the sake of consistency. <p>CA Ring:</p> <ul style="list-style-type: none"> • There were technical issues with the PBX environments that needed special attention. • There was also a problem with gateways and ports locking up and not providing any notification to the end user until they tried to dial out.
<i>Training</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> • The state formatted the call-taker screens to look as much like the old ones as possible to minimize the pain of transition. There was one day of training, followed by two shifts with a trainer present. They developed performance alerts that highlighted some of the areas of concern and reinforced the training and new features. State staff was in the PSAPs during implementation to support them through the transition. <p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> • Training is very important with over 5,000 telecommunicators. Training took place within two weeks of deployment and there was a trainer on site for the cut. The trainers supplemented with Job aid cards and have taken on most of the training responsibilities from the vendors. <p>NCTCOG:</p> <ul style="list-style-type: none"> • Classroom training in a central training facility was held within two weeks of a cut. A trainer was on site for the cut and all shifts that first day. Follow-up occurred two weeks later, making sure all questions were answered. On-line training updates and optional refresher training in the classroom for those that needed a little extra help rounded off the training process.

TOPIC	EARLY ADOPTER RESPONSES
	<p>State of Minnesota:</p> <ul style="list-style-type: none"> The NG advisory committee is under the statewide communications board. This committee has a subcommittee for training. They made the decision to contract with a community college for online interactive training modules and quizzes. <p>CA Ring:</p> <ul style="list-style-type: none"> Updates were pushed out to all telecommunicators and they cycled training across shifts. Training required paying some overtime. A vendor trainer had access (and used it) to make configuration changes that would conflict with our prime provider. This presented a challenge.
<i>Vendor Challenge</i>	<p>State of Iowa:</p> <ul style="list-style-type: none"> There were challenges between local CPE vendors and the network provider. Communications, finger pointing and notification issues from a middle man standpoint were a problem. <p>State of Minnesota:</p> <ul style="list-style-type: none"> There were challenges with coordination of resources and schedules with two different companies. There was also debate on whether the ESInet was an interstate or intrastate network.
Ongoing Operations	
<i>Maintenance</i>	<p>State of Maine:</p> <ul style="list-style-type: none"> The state has an emergency response center and that hasn't changed. However, a lesson learned was the need for well-documented procedures for notification of outages both to staff and each of the PSAPs. Monitoring and notification were other key lessons learned. It is very different from the legacy system. <p>Commonwealth of Massachusetts:</p> <ul style="list-style-type: none"> One of the requirements was a Network Operations Center (NOC) located in Massachusetts. None of the three bidders had this in place, but the trouble has been worth it to have local resources. The NOC was very useful during testing to see exactly what was happening in the network and fix it on the spot. The NOC is also responsible for on-going monitoring and alerts. A change management database and a ticketing system, complete with reporting were implemented. The Commonwealth extended maintenance contracts for the legacy system so it is maintained until the transition is complete. <p>Palm Beach County:</p> <ul style="list-style-type: none"> Procedures changed dramatically and staff is more involved. PSAPs used to just call the vendor with problems, but now the county is notified and engages to assist with every trouble ticket 24/7. Maintenance and monitoring has been the priority and the results have improved service in the region.

TOPIC	EARLY ADOPTER RESPONSES
	<p>NCTCOG:</p> <ul style="list-style-type: none"> Self-maintenance has improved service tremendously, according to surveys by the PSAPs. Staff and software have been a great investment in monitoring and notification, troubleshooting, resolution and preventative maintenance. <p>BRETSA:</p> <ul style="list-style-type: none"> BRETSA is increasing both internal and external type of monitoring notification system. They use a combination of third parties and internal design. They are very aggressive with security. BRETSA is also very good at collaboration. The chemistry between the team members, consultants, and the vendors has made the project successful. <p>State of Minnesota:</p> <ul style="list-style-type: none"> Procured a managed network with monitoring in the contract. The only complaint is that there have been too many notifications for all the small things that don't take down the network. There could be as many as 6 to 100 alarms in a single night. However, this is a decision that was made internally to be on the safe side. The requirements will be re-evaluated for the next contract. <p>CA Ring:</p> <ul style="list-style-type: none"> The vendors had to create some new monitoring processes and dive into their code to make sure they were having notifications sent with events that were identified. The changes made a big improvement in service.
<i>Resolving Issues</i>	<p>State of Iowa:</p> <ul style="list-style-type: none"> The state completed a master contract two years ago for CPE. Interoperability was tested with the network and the state gave the local service boards a list of vendors for procurement. They are working towards implementing text to 9-1-1 in the state with some standardized pricing. They are also using carryover funding to support PSAP grants for transitioning to NG9-1-1. So far, over \$10 million in PSAP equipment upgrades has been funded. <p>BRETSA:</p> <ul style="list-style-type: none"> One of the most important issues addressed was contingency planning. Adding this to the project made it take longer, but the board supported getting things done right. <p>State of Indiana:</p> <ul style="list-style-type: none"> Indiana was the first to implement outbound text from 9-1-1 in 2013. They use it as a tool for replying to hang up calls. Citizens were not answering the call backs from the PSAP from an unknown number. However, 80% will answer a text, saving on rolling responders when it is not necessary. The state is now working on statewide data collection and analytics. <p>State of Minnesota:</p> <ul style="list-style-type: none"> Developed a comprehensive communications plan in order to get every PSAP to volunteer to join the ESInet. Did not mandate participation. Went to each of the 7 regions and educated them and encouraged them to join – all did.

TOPIC	EARLY ADOPTER RESPONSES
<i>Billing/Additional Costs</i>	State of Minnesota: <ul style="list-style-type: none"> When the first bills were received, there were FUSFs (Federal Universal Service Fees) that the state had not been made aware of previously. They were applicable to an interstate network and because the IP SRs were out of state. It was unbudgeted and it increased costs as much as 20% on some elements.
<i>Contracts</i>	Commonwealth of Massachusetts: <ul style="list-style-type: none"> Contract language is vital to keeping change costs down and meeting requirements. One thing to improve on would be to add a provision to the contract that would allow a change in vendor personnel. The contract allowed a change in a technician, did not address a project or program manager if they were not meeting expectations.

7.2 Resources

Additional resources include:

Organization	Resource
FCC	Task Force on Optimal PSAP Architecture (TFOPA) First Report, Released February 19, 2016, at https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf
APCO	<ul style="list-style-type: none"> APCO Project 43 (http://psc.apcointl.org/2016/02/10/apco-launches-project-43-to-tackle-broadband-implications-for-the-psap/); APCO ProCHRT initiative (https://www.apcointl.org/resources/staffing-and-retention/professional-communications-human-resources-committee.html)
NENA	Training Guidelines - https://www.nena.org/page/trainingguidelines
The Industry Council	http://www.theindustrycouncil.org/policystatements/Final_G&R_Document_Submission.pdf
National 9-1-1 Program Office	http://www.9-1-1.gov/operationsandtraining.html

7.3 Acronyms

1G - First Generation (1G)
3GPP – Third Generation Partner Project
ACD - Automatic Call Distribution
ACM – Address Complete Message
ADA - Americans with Disabilities Act
ADR – Additional Data Repository
AES – Advanced Encryption Standard
AIP – Access Infrastructure Provider
ALI - Automatic Location Identification
ALRS – Agency Locator Record Store
ANI - Automatic Number Identification
ANSI – American National Standard Institute
APCO – Association of Public Safety Communications Officials
ATIS – Alliance for Telecommunications Industry Solutions
BCF - Border Control Functions
CAD - Computer Aided Dispatch
CAMA - Centralized Automatic Message Accounting
CAP – Common Alerting Protocol
CDR – Call Detail Record
CHS – Call Handling System
CIDB - Customer Information Data Bases
CJIS – Criminal Justice Information System
CLEC – Competitive Local Exchange Carrier
CoS – Class of Service
CPE - Customer Premise Equipment
CPE - Call Processing Equipment
CSRIC - Communications Security, Reliability and Interoperability Council's
DBMS - Database Management System
DES – Data Encryption Standard
DHCP – Dynamic Host Configuration Protocol
DHS – Department of Homeland Security
DNS - Domain Name Service
DNS - Directory Name Service
DOJ – Department of Justice
DoS – Denial of Service
DSL – Digital Subscriber Line
EC3 – Emergency Communications Cybersecurity Center
ECRF - Emergency Call Routing Function
EDXL – Emergency Data eXchange Language
EIDD – Emergency Incident Data Document
EMD - Emergency Medical Dispatch

EMS - Emergency Medical Services
ESInet - Emergency Services IP transport network
ESN - Emergency Services Numbers
ESRK – Emergency Services Routing Key
ESRP - Emergency Services Routing Proxy
FACA - Federal Advisory Committee Act
FCC - Federal Communications Commission
FE - Functional Elements
GCS – Geocode Service
GDP – Generic Digits Parameter
GIS - Geographic Information System
GML – Geography Markup Language
GMLC – Gateway Mobile Location Center
HELD – HTTP-Enabled Location Delivery Protocol
HTTP – HyperText Transfer Protocol
HVAC - Heating, Ventilating, and Air Conditioning
IaaS – Infrastructure-as-a-Service
IETF - Internet Engineering Task Force
IJIS – Information Justice Information Systems Institute
IM – Instant Message
IMR – Interactive Media Response
IMS – Internet Protocol Multimedia Subsystem
IoT - Internet of Things
IP - Internet Protocol
IPsec – Internet Protocol Security
IPSR - IP Selective Router
IRR - Instant Recall Recorder
ISDN – Integrated Services Digital Network
ISP – Internet Service Provider
IVR – Interactive Voice Response
LAN - Local Area Network
LATA - Local access and transport area
LEC - Local Exchange Carrier
LIF – Location Interwork Function
LIS - Location Information Server
LMR - Land Mobile Radio
LNG - Legacy Network Gateway
LO – Location Object
LoST - Location-to-Service Translation Protocol
LPG - Legacy PSAP Gateway
LRF – Location Retrieval Function
LSRG - Legacy Selective Router Gateway
LTE - Long Term Evolution

LVF - Location Validation Function
MCS – MSAG Conversion Service
MDN – Mobile Directory Number
MIS - Management Information System
MOUs - Memorandum of Understanding
MPC - Mobile Positioning Center
MSAG - Master Street Address Guide
MSRP – Message Session Relay Protocol
MSC – Mobile Switching Center
NANP – North American Numbering Plan
NCCIC – National Cybersecurity and Communications Integration Center
NCMEC - National Center for Missing and Exploited Children
NEMESIS - National Emergency Medical Services Information System
NENA - National Emergency Numbering Association
NG9-1-1 - Next Generation 9-1-1
NGCS - Next Generation Core Services
NG-SEC - Next Generation 9-1-1 Security
NIF – NG9-1-1 Specific Interwork Function
NIST – National Institute of Standards and Technology
NOC - Network Operating Centers
NSOC – Network Security Operations Center
NTP – Network Time Protocol
OGC – Open Geospatial Consortium
OSE - Originating Service Environments
OSP - Originating Service Providers
P25 - Project 25
PBX – Private Branch Exchange
PCA – PSAP Credentialing Agency
PIDF – Presence Information Data Format
PIDF-LO - Presence Information Data Format-Location Object
PIF – Protocol Interworking Function
POS - Point of Sale
PRF - Policy Routing Function
PSAP - Public Safety Answering Point
PSP – Provisioning Service Provider
PSTN - Public Switched Telephone Network
PTSD - Post-Traumatic Stress Disorder
QA - Quality Assurance
QC - Quality Control
QOS - Quality of Service
RFC – Request-for-Comment
RMS - Records Management System
ROI - Return-on-Investment

RTP – Real Time Protocol
RTT – Real Time Text
SaaS – Software-as-a-Service
SBC - Sessions Border Controller
SI – Spatial Interface
SIP – Session Initiated Protocol
SLA - Service Level Agreement
SMS – Short Message Service
SNMP - Simple Network Management Protocol
SOC – Security Operations Center
SOI – Service Order Interface
SOAP – Simple Object Access Protocol
SOP - Standard Operating Procedures
SR - Selective Router / Selective Routing
SRDB - Selective Routing Database
SS7 - Signaling System 7
TDD – Telecommunications Device for the Deaf and Hearing Impaired (aka TTY)
TDM – Time Division Multiplexing
TFOPA - Task Force on Optimal PSAP Architecture
TN - Telephone Number
TTY – Teletypewriter (aka TDD)
URI - Uniform Resource Identifier
URL – Uniform Resource Locator
URN – Uniform Resource Name
USPS - US Postal Service
VMM - Value Measuring Methodology (VMM)
VoIP - Voice over Internet Protocol
VPC - VoIP Positioning Center
VPN – Virtual Private Network
VSPs - VoIP Service Providers
WAN - Wide Area Network
XML – Extensible Markup Language

7.4 Glossary of Terms

The following glossary of terms is an enhanced version of that published in NENA Detailed Functional and Interface Standards for the NENA i3 Solution, NENA-STA-010.2-2016 (September 10, 2016).³³

Term	Definition / Description
3GPP (3RD Generation Partner Project)	The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies which are known as “Organizational Partners”. (http://www.3gpp.org/)
3GPP2 (3rd Generation Partnership Project 2)	A collaborative third generation (3G) telecommunications specifications-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 Cellular Radio telecommunication Intersystem Operations network evolution to 3G and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. A sister project to 3GPP.
9-1-1 Authority/Body	A State, County, Regional or other governmental entity responsible for 9-1-1 service operations. For example, this could be a county/parish or city government, a special 9-1-1 or Emergency Communications District, a Council of Governments or other similar body. (Source: NENA Master Glossary)
ACK (Acknowledgement)	A message to indicate the receipt of data.
ACM (Address Complete Message)	An ISDN (Integrated Services Digital Network) User Part (ISUP) message returned from the terminating switch when the subscriber is reached and the phone starts ringing, or when the call traverses an interworking point and the intermediate trunk is seized.
Additional Data	Data that further describe the nature of how the call was placed, the person(s) associated with the device placing the call, or the location the call was placed from.
Administrator	A person whose job is to manage a company, school, or other organization (http://www.merriam-webster.com/dictionary/administrator)
ADR (Additional Data Repository)	A data storage facility for Additional Data. The ADR dereferences a URI passed in a Call-Info header field or PIDF-LO <provided-by> and returns an Additional Data object block. It replaces and deprecates the concept of CIDB previously defined in 08-003 v1
AES (Advanced Encryption Standard)	A Federal Information Processing Standard (FIPS)-approved cryptographic algorithm that is used to protect electronic data.
Agency	In NG9-1-1, an organization that is connected directly or indirectly to the ESInet. Public safety agencies are examples of Agency. An

³³ NENA, Detailed Functional and Interface Standards for the NENA i3 Solution, http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/standards/NENA-STA-010.2_i3_Architectu.pdf. For a complete glossary of terms, see NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000, <https://www.nena.org/?page=Glossary>.

Term	Definition / Description
	entity such as a company that provides a service in the ESInet can be an Agency. Agencies have identifiers and credentials that allow them access to services and data.
Agent	In NG9-1-1, an Agent is an authorized person - employee, contractor or volunteer, who has one or more roles, in an Agency. An Agent can also be an automaton in some circumstances (e.g. an IMR answering a call)
AIP (Access Infrastructure Provider)	The entity providing physical communications access to the subscriber. This access may be provided over telco wire, CATV cable, wireless or other media. Usually, this term is applied to purveyors of broadband internet access but is not exclusive to them.
ALRS (Agency Locator Record Store)	A web service that, when presented with an agency locator URI, returns the agency locator record.
AMR (Adaptive Multi Rate (codec))	An audio compression format optimized for speech coding that automatically changes coding rates in response to the input audio stream.
AMR-WB (Adaptive Multi Rate (codec) – Wide Band)	An audio compression format optimized for wideband speech coding that automatically changes coding rates in response to the input audio stream.
ANI (Automatic Number Identification)	Telephone number associated with the access line from which a call originates
ANSI (American National Standards Institute)	Entity that coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. Please refer to: http://www.ansi.org
APCO (Association of Public Safety Communications Officials)	APCO is the world's oldest and largest not-for-profit professional organization dedicated to the enhancement of public safety communications
ATIS (Alliance for Telecommunications Industry Solutions)	A U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Please refer to: http://www.atis.org Ref: NENA 03-507 Ref: NENA 08-002 Ref: NENA 08-504 Ref: NENA 57-502
B2BUA (Back to Back User Agent)	A back to back user agent is a SIP element that relays signaling mechanisms while performing some alteration or modification of the messages that would otherwise not be permitted by a proxy server. A logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server it maintains dialog state and must participate in all requests sent on the dialogs it established.

Term	Definition / Description
BCF (Border Control Function)	Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet
BISACS (Building Information Services And Control System)	A computer based system that allows access to building information such as its structural layout and/or to monitor a particular building or set of buildings for alerts
CAMA (Centralized Automatic Message Accounting)	A type of in-band analog transmission protocol that transmits telephone number via multi-frequency encoding. Originally designed for billing purposes.
CAP (Common Alerting Protocol)	The Common Alerting Protocol is a general format for exchanging emergency alerts, primarily designed as an interoperability standard for use among warning systems and other emergency information systems.
CDR (Call Detail Record)	A record stored in a database recording the details of a received or transmitted call (from 08-003). The data information sent to the ALI computer by a remote identifying device (PBX, Call Position Identifier, ...)
cid (Content Identifier (Content-ID))	An identifier used to refer to a Multipurpose Internet Mail Extensions (MIME) block
CIDB (Call Information Database (obsolete, replaced with Additional Data Repository))	Obsolete, see Additional Data Repository
Codec (COder/DECoder)	In communications engineering, the term codec is used in reference to integrated circuits, or chips that perform data conversion. In this context, the term is an acronym for “coder/decoder.” This type of codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. In personal and business computing applications, the most common use for such a device is in a modem.
CoS (Class of Service)	A designation in E9-1-1 that defines the service category of the telephony service. Examples are residential, business, Centrex, coin, PBX, VoIP and wireless Phase II (WPH2). Ref: NENA 02010 Ref: NENA 02-011
CPE (Customer Premises Equipment)	Communications or terminal equipment located in the customer’s facilities – Terminal equipment at a PSAP.
Dereference	The act of exchanging a reference to an item by its value. For example the dereference operation for location uses a protocol such as SIP or HELD to obtain a location value (PIDF-LO).
DES (Data Encryption Standard)	The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys, i.e., one for encryption and one for decryption.

Term	Definition / Description
DHCP (Dynamic Host Control Protocol (i2) Dynamic Host Configuration Protocol)	Dynamic Host Configuration Protocol) A widely used configuration protocol that allows a host to acquire configuration information from a visited network and, in particular, an IP address.
DNS (Domain Name Server (or Service or System))	Used in the Internet today to resolve domain names. The input to a DNS is a domain name (e.g., telcordia.com); the response is the IP address of the domain. The DNS allows people to use easy to remember text-based addresses and the DNS translates those names into routable IP addresses.
DoS (Denial of Service)	A type of cyber-attack intended to overwhelm the resources of the target and deny the ability of legitimate users of the target the normal service the target provides
DSL (Digital Subscriber Line)	A “last mile” solution that uses existing telephony infrastructure to deliver high speed broadband access. DSL standards are administered by the DSL Forum (http://dslforum.org/)
E9-1-1 (Enhanced 9-1-1)	A telephone system which includes network switching, database and Public Safety Answering Point premise elements capable of providing automatic location identification data, selective routing, selective transfer, fixed transfer, and a call back number. The term also includes any enhanced 9-1-1 service so designated by the Federal Communications Commission in its Report and Order in WC Docket Nos. 04-36 and 05-196, or any successor proceeding.
ECRF (Emergency Call Routing Function)	A functional element in an ESInet which is a LoST protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller’s location or towards a responder agency.
EDXL (Emergency Data eXchange Language)	The Emergency Data Exchange Language (EDXL) is a broad initiative to create an integrated framework for a wide range of emergency data exchange standards to support operations, logistics, planning and finance.
EIDD (Emergency Incident Data Document)	A National Information Exchange Model (NIEM) conformant object that is used to share emergency incident information between and among authorized entities and systems
ESInet (Emergency Services IP Network)	An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based internetwork (network of networks). The term ESInet designates the network, not the services that ride on the network. See NG9-1-1 Core Services.

Term	Definition / Description
ESN (Emergency Service Number, Electronic Serial Number, Emergency Service Network)	A 3-5 digit number that represents one or more ESZs. An ESN is defined as one of two types: Administrative ESN and Routing ESN.
ESRK (Emergency Services Routing Key)	Either a 10-digit North American Numbering plan or non-NANPA number that uniquely identifies a wireless emergency call, is used to route the call through the network, and used to retrieve the associated ALI data. In the past, these numbers may have been dialable or non-dialable. As of 2012 these numbers should be non-dialable, and all new ESRKs will be non-NANPA, non-dialable ten-digit numbers.
ESRP (Emergency Service Routing Proxy)	An i3 functional element which is a SIP proxy server that selects the next hop routing within the ESInet based on location and policy. There is an ESRP on the edge of the ESInet. There is usually an ESRP at the entrance to an NG9-1-1 PSAP. There may be one or more intermediate ESRPs between them.
EVRC (Enhanced Variable Rate Codec)	A speech codec developed to offer mobile carriers more network capacity while not increasing bandwidth requirements.
EVRC-WB (Enhanced Variable Rate Wideband Codec)	A speech codec providing enhanced (wideband) voice quality
FAC (Facility (SS7 message))	A message sent in either direction at any phase of the call to request an action at another exchange.
FCC (Federal Communications Commission)	An independent U.S. government agency overseen by Congress, the Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories
FCI (Feature Code Indicator)	Information sent in either direction to invoke a specific feature operation at the terminating or originating switch,
FE (Functional Element)	An abstract building block that consists of a set of interfaces and operations on those interfaces to accomplish a task. Mapping between functional elements and physical implementations may be one-to-one, one-to-many or many-to-one.
FQDN (Fully Qualified Domain Name)	The complete domain name for a specific computer, or host, on the Internet.
g.711 a-law	An ITU-T Recommendation for an audio codec for telephony in non-North American regions
g.711 mu-law	An ITU-T Recommendation for an audio codec for telephony in the North American region.
GCS (Geocode Service)	An NG9-1-1 service providing geocoding and reverse-geocoding
GDP (Generic Digits Parameter)	Identifies the type of address to be presented in calls set up or additional numeric data relevant to supplementary services such as LNP or E91-1.

Term	Definition / Description
Geopriv (Geographic Location/Privacy)	The name of an IETF work group, now dormant, which created location representation formats such as PIDF-LO and protocols for transporting them, such as HELD used in NG9-1-1.
GeoRSS (Geodetic Really Simple Syndication)	A simple mechanism used to encode GML in RSS feeds for use with the ATOM protocol
Geoshape (Geodetic Shape)	One of a list of shapes defined originally by the IETF and standardized by the Open Geospatial Consortium that can be found in a PIDF-LO. Includes point, circle, ellipse, arc band, polygon, and 3D versions of same.
GIS (Geographic Information System)	A system for capturing, storing, displaying, analyzing and managing data and associated attributes which are spatially referenced
GML (Geography Markup Language)	An XML grammar for expressing geographical features standardized by the OGC
GRUU (Globally Routable User agent URI)	A SIP URI which identifies a specific endpoint where a user is signed on that is routable on the Internet
H.264/MPEG-4	An ITU-T Recommendation and Motion Picture Expert Group standard for a video codec
HELD (HTTP-Enabled Location Delivery Protocol)	A protocol that can be used to acquire Location Information (LI) from a LIS within an access network as defined in IETF RFC 5985.
HTTP (HyperText Transfer Protocol)	Hypertext Transport protocol typically used between a web client and a web server that transports HTML and/or XML.
HTTPS (HyperText Transfer Protocol Secure)	HTTP with secure transport (Transport Layer Security or its predecessor, Secure Sockets Layer)
I3 PSAP Multimedia Call Handling System	A 9-1-1 multimedia call handling system as defined in Section 3-Operational or Technical Description of NENA/APCO-REQ-001.1.1-2016, NENA/APCO Next Generation 9-1-1 Public Safety Answering Point Requirements.
IAM (Initial Address Message)	First message sent to inform the partner switch that a call has to be established on the CIC contained in the message. Contains the called number, type of service (speech or data) and optional parameters.
IANA (Internet Assigned Numbers Authority)	IANA is the entity that oversees global IP address allocation; DNS root zone management, and other Internet protocol assignments.
ICE (Interactive Connectivity Establishment)	A mechanism for endpoints to establish RTP connectivity in the presence of NATs and other middle boxes.
IDP (Identity Provider)	An entity which authenticates users and supplies services with a “token” that can be used in subsequent operations to refer to an authorized user.
IETF (Internet Engineering Task Force)	Lead standard setting authority for Internet protocols.
IM (Instant Messaging)	A method of communication generally using text where more than a character at a time is sent between parties nearly instantaneously

Term	Definition / Description
IMR (Interactive Media Response)	An automated service used to play announcements, record responses and interact with callers using any or all of audio, video and text
IMS (Internet Protocol Multimedia Subsystem)	The IP Multimedia Subsystem comprises all 3GPP/3GPP2 core network elements providing IP multimedia services that support audio, video, text, pictures alone or in combination delivered over a packet switched domain.
Incident Tracking Identifier	An identifier assigned by the first element in the first ESInet that handles an emergency call or declares an incident. Incident Tracking Identifiers are globally unique.
INVITE	A SIP transaction used to initiate a session (See re-INVITE).
IP (Internet Protocol)	The method by which data is sent from one computer to another on the Internet or other networks.
IPsec (Internet Protocol Security)	IPsec is the next-generation network layer crypto platform. IPsec can be found on routers, firewalls, and client desktops.
IPv4 (Internet Protocol version 4)	The fourth version of the Internet Protocol; uses 32-bit addresses
IPv6 (Internet Protocol version 6)	The most recent version of the Internet Protocol; uses 128-bit addresses.
IS-ADR (Identity Searchable Additional Data Repository)	An Additional Data Repository that provides a service that can search for Additional Data based on a sip/sips or tel URI: (e.g., Additional Data about the caller).
ISDN (Integrated Services Digital Network)	International standard for a public communication network to handle circuit-switched digital voice, circuit-switched data, and packet-switched data.
ISP (Internet Service Provider)	A company that provides Internet access to other companies and individuals.
ISUP (Integrated Services Digital Network User Part)	A message protocol to support call set up and release for interoffice voice call connections over SS7 Signaling.
ITU (International Telecommunication Union)	The telecommunications agency of the United Nations established to provide worldwide standard communications practices and procedures. Formerly CCITT.
KP (Key Pulse)	An MF signaling tone (digit)
LIF (Location Interwork Function)	The functional component of a Legacy Network Gateway which is responsible for taking the appropriate information from the incoming signaling (i.e., calling number/ANI, ESRK, cell site/sector) and using it to acquire location information that can be used to route the emergency call and to provide location information to the PSAP. In a Legacy PSAP Gateway, this functional component takes the information from an ALI query and uses it to obtain location from a LIS.
LIS (Location Information Server)	A Location Information Server (LIS) is a functional element that provides locations of endpoints. A LIS can provide Location-by-Reference, or Location-by-Value, and, if the latter, in geodetic or

Term	Definition / Description
	civic forms. A LIS can be queried by an endpoint for its own location, or by another entity for the location of an endpoint. In either case, the LIS receives a unique identifier that represents the endpoint, for example an IP address, circuit-ID or MAC address, and returns the location (value or reference) associated with that identifier. The LIS is also the entity that provides the dereferencing service, exchanging a location reference for a location value.
LNG (Legacy Network Gateway)	An NG9-1-1 Functional Element that provides an interface between an un-upgraded legacy origination network and the NGCS.
LO (Location Object)	<p>In an emergency calling environment, the LO is used to refer to the current position of an endpoint that originates an emergency call. The LO is expected to be formatted as a Presence Information Data Format – Location Object (PIDF-LO) as defined by the IETF in RFC 4119, updated by RFCs 5139, 5491 and 7459, and extended by RFC 6848. The LO may be:</p> <ul style="list-style-type: none"> • Geodetic – shape, latitude(s), longitude(s), elevation, uncertainty, confidence and the datum which identifies the coordinate system used. NENA prescribes that geodetic location information will be formatted using the World Geodetic System 1984 (WGS 84) datum; • Civic location – a set of elements describing detailed street address information. For NG9-1-1 in the U.S., the civic LO must conform to NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF) Standard (NENA-STA-004); <p>Or a combination thereof.</p>
LoST (Location to Service Translation)	A protocol that takes location information and a Service URN and returns a URI. Used generally for location-based call routing. In NG9-1-1, used as the protocol for the ECRF and LVF.
LPG (Legacy PSAP Gateway)	An NG9-1-1 Functional Element which provides an interface between an ESInet and an un-upgraded PSAP
LRF (Location Retrieval Function)	The IMS associated functional entity that handles the retrieval of location information for the emergency caller including, where required, interim location information, initial location information and updated location information. The LRF may interact with a separate RDF or contain an integrated RDF in order to obtain routing information for an emergency call.
LSRG (Legacy Selective Router Gateway)	The LSRG provides an interface between a 9-11 Selective Router and an ESInet, enabling calls to be routed and/or transferred between Legacy and NG networks. A tool for the transition process from Legacy 9-1-1 to NG9-1-1.
LVF (Location Validation Function)	A functional element in an NGCS that is a LoST protocol server where civic location information is validated against the authoritative GIS database information. A civic address is considered valid if it can be located within the database uniquely, is suitable to provide an accurate route for an emergency call and adequate and specific enough to direct responders to the right location.

Term	Definition / Description
MCS (MSAG Conversion Service)	A web service providing conversion between PIDsF-LO and MSAG data.
MDN (Mobile Directory Number)	The telephone number dialed to reach a wireless telephone.
MF (Multi-Frequency)	A type of in-band signaling used on analog interoffice and 9-1-1 trunks.
MIB (Management Information Base)	An object used with the Simple Network Management Protocol to manage a specific device or function
MIME (Multipurpose Internet Mail Extensions)	A specification for formatting non-ASCII messages so that they can be sent over the Internet.
MPC/GMLC (Mobile Positioning Center/ Gateway Mobile Location Center)	The MPC/GMLC serves as the point of interface to the ANSI wireless network for the Emergency Services Network. The MPC/GMLC serves as the entity which retrieves forwards, stores and controls position data within the location network. It can select the PDE(s) to use in position determination and forwards the position to the requesting entity or stores it for subsequent retrieval. In the case of a PDE with autonomous determination capability, the MPC/GMLC receives and stores the position estimation for subsequent retrieval. The MPC/GMLC may restrict access to position information (e.g., require that the Mobile Station be engaged in an emergency service call or only release position information to authorized nodes.)
MSAG (Master Street Address Guide)	A database of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 9-1-1 calls.
MSC (Mobile Switching Center)	The wireless equivalent of a Central Office, which provides switching functions from wireless calls
MSRP (Message Session Relay Protocol)	A standardized mechanism for exchanging instant messages using SIP where a server relays messages between user agents.
MTP (Message Transfer Part)	A layer of the SS7 protocol providing the routing and network interface capabilities to support call setup.
NANP (North American Numbering Plan)	An integrated telephone numbering plan serving 20 North American countries that share telephone numbers in the +1 country code
NAPT (Network Address and Port Translation)	A methodology of remapping one IP address and port into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
NAT (Network Address Translation)	A methodology of remapping one IP address into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
NCCIC (National Cybersecurity and Communications Integration Center)	Part of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) (formerly referred to as US-CERT) serves as a central location

Term	Definition / Description
	where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts. Ref: https://www.us-cert.gov/nccic
NENA (National Emergency Number Association)	Professional organization focused on 9-1-1 policy, technology, operations, and education issues. NENA works with public policy leaders; emergency services and telecommunications industry partners to facilitate the creation of an IP-based Next Generation 9-1-1 system; and to establish industry leading standards, training, and certifications.
NG9-1-1 (Next Generation 9-1-1)	NG9-1-1 is an Internet Protocol (IP)-based system comprised of managed Emergency Services IP networks (ESInets), functional elements (applications), databases, and call handling systems (CHS) that replicate traditional E9-1-1 features and functions and provides additional capabilities. NG9-1-1 is designed to provide access to emergency services from all connected communications sources, and provide multimedia data capabilities for Public Safety Answering Points (PSAPs) and other emergency service organizations.
NGCS (Next Generation 9-1-1 (NG9-1-1) Core Services)	The base set of services needed to process a 9-1-1 call on an ESInet. Includes the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network
NIF (NG9-1-1 Specific Interwork Function)	The functional component of a Legacy Network Gateway or Legacy PSAP Gateway which provides NG9-1-1-specific processing of the call not provided by an off-the-shelf protocol interwork gateway.
NPD (Numbering Plan Digit)	A component of the traditional 8-digit 9-1-1 signaling protocol between the Enhanced 9-1-1 Control Office and the PSAP CPE. Identifies 1 of 4 possible area codes.
NRS (NENA Registry System)	The entity provided by NENA to manage registries.
NTP (Network Time Protocol)	A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
OASIS (Organization for the Advancement of Structured Information Standards)	An organization that promulgates standards for data interchange
OGC (Open Geospatial Consortium)	An organization that promulgates standards for the global geospatial community
Originating ESRP	The first routing element inside the NGCS. It receives calls from the BCF at the edge of the ESInet.

Term	Definition / Description
OSI (Open Systems Interconnection)	A 7-layer hierarchical reference model structure developed by the International Standards Organization for defining, specifying, and relating communications protocols; not a standard or a protocol; Layer Description – (7) Application Provides interface with network users, (6) Presentation Performs format and code conversion, (5) Session Manages connections for application programs, (4) Transport Ensures end-to-end delivery, (3) Network Handles network addressing and routing, (2) Data Link Performs local addressing and error detection and (1) Physical Includes physical signaling and interfaces.
P-A-I (P-Asserted-Identity)	A header in a SIP message containing a URI that the originating network asserts is the correct identity of the caller.
PCA (PSAP Credentialing Agency)	The root authority designated to issue and revoke security credentials (in the form of an X.509 certificate) to authorized 9-1-1 agencies in an ESIInet.
PIDF (Presence Information Data Format)	The Presence Information Data Format is specified in IETF RFC 3863; it provides a common presence data format for Presence protocols, and also defines a new media type. A presence protocol is a protocol for providing a presence service over the Internet or any IP network.
PIDF-LO (Presence Information Data Format – Location Object)	Provides a flexible and versatile means to represent location information in a SIP header using an XML schema.
PIF (Protocol Interworking Function)	That functional component of a Legacy Network Gateway or Legacy PSAP Gateway that interworks legacy PSTN signaling such as ISUP or CAMA with SIP signaling.
PKI (Public Key Infrastructure)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Precedent	Refers to those items that require the existence of others that have been completed "prior in time, order, arrangement, or significance" (Source: Miriam Webster Dictionary)
PRF (Policy Routing Function)	That functional component of an Emergency Service Routing Proxy that determines the next hop in the SIP signaling path using a policy.
PSAP (Public Safety Answering Point)	Public Safety Answering Point (PSAP): An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy. Note: PSAPs referred to in this document are those operated by local and state government. Some states include federally operated PSAPs (such as those operated by Dept. of Interior and Defense) and those operated by Tribal Nations, but this practice is not consistent or universal.
PSP (Provisioning Service Provider)	The component in an ESIInet functional element that implements the provider side of a SPML interface used for provisioning

Term	Definition / Description
PSTN (Public Switched Telephone Network)	The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.
QoS (Quality of Service)	As related to data transmission a measurement of latency, packet loss and jitter
REFER/Replaces	Use of the SIP REFER method together with a Replaces header as part of a transfer operation to indicate that a new leg is to be created that replaces an existing call leg.
Regional	Defined as either intrastate or interstate
re-INVITE	A SIP INVITE transaction within an established session used to change the parameters of a call or refresh a session. See INVITE.
REL (Release (message))	An ISUP message sent in either direction to release the circuit.
RequestURI	That part of a SIP message that indicates where the call is being routed towards. SIP Proxy servers commonly change the Request ID (“retargeting”) to route a call towards the intended recipient.
Resource Priority	A header used on SIP calls to indicate priority that proxy servers give to specific calls. The Resource Priority header does not indicate that a call is an emergency call (see RequestURI).
REST (Representational State Transfer)	An interface that transmits domain-specific data over HTTP without an additional messaging layer such as SOAP or session tracking via HTTP cookies.
RFC (Request for Comment)	A method by which standard setting bodies receive input from interested parties outside of the working group.
RLC (Release Complete (message))	An ISUP message sent to acknowledge the release (REL) message indicating that the circuit is idle afterward and can be used again.
ROH (Receiver Off-Hook)	A call state in which the recipient’s hand set is not in the cradle.
ROHC (Robust Header Compression)	A standardized method to compress the IP, UDP, UDP-Lite, RTP, and TCP headers of Internet packets.
RTCP (Real-time Transport Control Protocol)	RTCP is a sister protocol of RTP and provides out-of-band control information for an RTP flow. It partners RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP. It gathers statistics on a media connection and information such as bytes sent, packets sent, lost packets, jitter, feedback and round trip delay. An application may use this information to increase the quality of service perhaps by limiting flow, or maybe using a low compression codec instead of a high compression codec. RTCP is used for Quality of Service (QoS) reporting.
RTP (Real Time Protocol)	An IP protocol used to transport media (voice, video, text) which has a real time constraint.

Term	Definition / Description
RTSP (Real Time Streaming Protocol)	A network control protocol designed for use in entertainment and communications systems to control streaming media servers.
RTT (Real Time Text)	Text transmission that is character at a time, as in TTY.
SAML (Security Assertion Markup Language)	An XML-based, open-standard data format for exchanging authentication and authorization data between an identity provider and another party
SAP (Service Activation Parameter)	A parameter included in an SS7 call control message to invoke an action at another node or report the result of such an action.
SCTP (Stream Control Transport Protocol)	SCTP is defined by IETF RFC2960 as the transport layer to carry signaling messages over IP networks. SCTP/T is just one of the many products in the Adax Protocol Software (APS) SIGTRAN suite that has been designed for Convergence, Wireless and Intelligent Networks. Compliant with IETF RFC2960 and RFC3309, SCTP/T (SCTP for Telephony) is implemented in the OS kernel. SCTP/T provides a transport signaling framework for IP networks that enhances the speed and capability of SSCS/HSL and can be deployed over T1/E1, Ethernet and ATM OC3 physical media interfaces. In addition to the services specified in IETF RFC2960, Adax SCTP/T also provides a transport framework with levels of service quality and reliability as those expected from a Public Switched Telephone Network (PSTN).
SDO (Standards Development Organization)	An entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining standards that address the interests of a wide base of users outside the standards development organization.
SDP (Session Description Protocol)	A standard syntax contained in a signaling message to negotiate a real time media session. See RFC4566.
Security Posture	An event that represents a downstream entity's current security state (normal, under attack ...).
Service Uniform Resource Name (Service URN)	A URN with "service" as the first component supplied as an input in a LoST request to an ECRF to indicate which service boundaries to consider when determining a response. A Request URI with the service URN of "urn:service:sos" is used to mark a call as an emergency call. See RequestURI.
SHA (Secure Hash Algorithm)	One of a number of fixed-size, cryptographic algorithms promulgated by the National Institute of Standards and Technology used to provide integrity protection for messages, files and other data objects.
SI (Spatial Interface)	A standardized interface between the GIS and the functional elements that consume GIS data, such as the ECRF/LVF
SIO (Service Information Octet)	An eight-bit data field that is present in an SS7 message signal unit and is comprised of the service indicator and the sub-service field. It is used to determine the user part to which an incoming message should be delivered

Term	Definition / Description
SIP (Session Initiation Protocol)	An IETF defined protocol (RFC3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, i2 and i3
SLA (Service Level Agreement)	A contract between a service provider and the end user, which stipulates and commits the service provider to a required level of service.
SMS (Short Message Service)	A service typically provided by mobile carriers that sends short (160 characters or fewer) messages to an endpoint. SMS is often fast, but is not real time.
SNMP (Simple Network Management Protocol)	A protocol defined by the IETF used for managing devices on an IP network.
SOA (Service Oriented Architecture)	A model in computer software design in which application components provide a repeatable business activity to other components using a communications protocol, typically over a network.
SOAP (Simple Object Access Protocol)	SOAP is a protocol for exchanging XML-based messages over a computer network, normally using HTTP. SOAP forms the foundation layer of the Web services stack, providing a basic messaging framework that more abstract layers can build on
SOS URN	A service URN starting with “urn:service:sos” which is used to mark calls as emergency calls as they traverse an IP network and to specify the desired emergency service in an ECRF request. See Service Uniform Resource Name.
SR (Selective Router [a.k.a., E9-1-1 Tandem, or Enhanced 9-1-1 (E9-1-1) Control Office])	The Central Office switch that provides the tandem switching of 9-1-1 calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP
SR (Selective Routing)	The process by which 9-1-1 calls/messages are routed to the appropriate PSAP or other designated destination, based on the caller’s location information, and may also be impacted by other factors, such as time of day, call type, etc. Location may be provided in the form of an MSAG-valid civic address or in the form of geo coordinates (longitude and latitude). Location may be conveyed to the system that performs the selective routing function in the form of ANI or pseudo-ANI associated with a pre-loaded ALI database record (in Legacy 9-1-1 systems), or in real time in the form of a Presence Information Data Format – Location Object (PIDF-LO) (in NG9-1-1 systems) or whatever forms are developed as 9-1-1 continues to evolve.
SRTP (Secure Real Time Protocol)	An IP protocol used to securely transport media (voice, video, text) which have a real time constraint.
SRV (Service [a DNS record type])	A specification of data in the Domain Name System defining the location, i.e. the hostname and port number, of servers for specified services.

Term	Definition / Description
SS7 (Signaling System 7)	An out-of-band signaling system used to provide basic routing information, call set-up and other call termination functions. Signaling is removed from the voice channel itself and put on a separate data network.
State	Includes all states, commonwealths and territories
TCP (Transmission Control Protocol)	A communications protocol linking different computer platforms across networks. TCP/IP functions at the 3rd and 4th levels of the open system integration model.
TDM (Time Division Multiplexing)	A digital multiplexing technique for combining a number of signals into a single transmission facility by interweaving pieces from each source into separate time slots.
Terminating ESRP	The last ESRP involved in call delivery, the terminating ESRP typically chooses the queue of call takers into which the call is delivered.
TLS (Transport Layer Security)	An Internet protocol that operates between the IP layer and TCP and provides hop-by-hop authentication, integrity protection and privacy using a negotiated cipher-suite.
TN (Telephone Number)	A sequence of digits assigned to a device to facilitate communications via the public switched telephone network or other private network.
TRD (Technical Requirements Document)	NENA Technical Requirements Document, developed by a Technical Committee, is used as basis for a NENA Technical Committee or outside Standards Development Organization (SDO) to develop formal industry accepted standards or guidelines
TTY (Teletypewriter [a.k.a. TDD, Telecommunications Device for the Deaf and Hard-of-Hearing])	In 9-1-1, a device that uses a keyboard and display, and communicating with tone signaled Baudot or ASCII.
TURN (Traversal Using Relays Around NAT)	A mechanism for establishing RTP connections through some kinds of NAT devices that won't allow two endpoints to connect directly. TURN uses a relay outside the NAT boundaries
TYS (Type of Service)	A designation in E9-1-1 that specifies if caller's service is published or non-published and if it is a foreign exchange outside the E9-1-1 serving area. Ref: NENA 02-010 Ref: NENA 02-011
UA (User Agent)	As defined for SIP in IETF RFC 3261[5], the User Agent represents an endpoint in the IP domain, a logical entity that can act as both a user agent client (UAC) that sends requests, and as user agent server (UAS) responding to requests.
UAC (User Agent Client)	Refer to IETF RFC 3261 for the following definition. "A user agent client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction."

Term	Definition / Description
UAS (User Agent Server)	Refer to IETF RFC 3261 for the following definition. “A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction.”
UDDI Universal Description, Discovery and Integration	An XML-based registry for businesses worldwide, which enables businesses to list themselves and their services on the Internet
UDP (User Datagram Protocol)	One of several core protocols commonly used on the Internet. Used by programs on networked computers to send short messages, called datagrams, between one another. UDP is a lightweight message protocol, compared to TCP, is stateless and more efficient at handling lots of short messages from many clients compared to other protocols like TCP. Because UDP is widely used, and also since it has no guaranteed delivery mechanism built in, it is also referred to as Universal Datagram Protocol, and as Unreliable Datagram Protocol.
URI (Uniform Resource Identifier)	A predictable formatting of text used to identify a resource on a network (usually the Internet) or a string of characters that must follow prescribed syntaxes such as URL, URN... Note Version 1.1 of the XML namespaces recommendation uses IRIs (Internationalized Resource Identifiers) instead of URIs. However, because version 1.1 is not yet a full recommendation [February, 2003] and because the IRI RFC is not yet complete, this document continues to refer to URIs instead of IRIs.
URL (Uniform Resource Locator [location sensitive])	A URL is a URI specifically used for describing and navigating to a resource (e.g. http://www.nena.org)
URN (Uniform Resource Name [location insensitive])	Uniform Resource Identifiers (URIs) that use the URN scheme, and are intended to serve as persistent, location-independent resource names.
USPS (United States Postal Service)	An independent agency of the United States government responsible for providing mail service in the United States.
UTC (Universal Coordinated Time)	The primary time standard in the world based on the time zone in Greenwich.
VEDS (Vehicle Emergency Data Sets)	A uniform data set for the collection and transmission of Advanced Automatic Collision Notification (AACN) data by automotive Telematics Service Providers (TSPs).
VESA (Valid Emergency Services Authority)	This organization is the root source of all certificates. It is responsible for identifying and issuing certificates either directly to end using entities or through delegate credential authorities. It is responsible for ensuring that any delegate credential authority that it identifies is properly qualified and operating with sufficient security and legitimacy to perform this role. Where VESA issues certificates directly to end users, it also has the responsibilities of a delegate credential authority in those cases.

Term	Definition / Description
VoIP (Voice over Internet Protocol)	Technology that permits delivery of voice calls and other real-time multimedia sessions over IP networks.
VPN (Virtual Private Network)	A network implemented on top of another network, and private from it, providing transparent services between networks or devices and networks. VPNs often use some form of cryptographic security to provide this separation.
VSP (VoIP Service Provider)	A company that offers VoIP telecommunications services that may be used to generate a 9-1-1 call, and interconnects with the 9-1-1 network.
WFS (Web Feature Service)	A web service that allows a client to retrieve and update geospatial data encoded in Geography Markup Language (GML).
WSDL (Web Service Definition Language)	An XML-based interface definition language that is used for describing the functionality offered by a web service.
X.509	An ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). In NG9-1-1, refers to the format of a certificate containing a public key.
XML (eXtensible Markup Language)	An internet specification for web documents that enables tags to be used that provide functionality beyond that in Hyper Text Markup Language (HTML). Its reference is its ability to allow information of indeterminate length to be transmitted to a PSAP call taker or dispatcher versus the current restriction that requires information to fit the parameters of pre-defined fields.
XMPP (Extensible Messaging and Presence Protocol)	A standardized protocol for exchanging instant messages, presence, files and other objects.