NENA Request for Proposal Considerations Information Document

Abstract: This document will assist 9-1-1 Authorities in developing an RFP to procure elements of an NG9-1-1 system, including PSAP Functional Elements (FE), NG9-1-1 Core Services, Geographic Information System (GIS) Data and Services, and Management Information System (MIS) Data Collection and Reporting.

NENA Request for Proposal Considerations Information Document

NENA-INF-021.2-2026
DSC Approval: June 23, 2026
PRC Approval: August 7,2026
NENA Board of Directors Approval: August 12, 2026
Next Scheduled Review Date: November 2026

Prepared by:
National Emergency Number Association (NENA), PSAP Logistics Committee, RFP Working Group

1 Executive Overview

The Request for Proposal (RFP) Considerations Information Document is intended for 9-1-1 Authorities or the consultants providing procurement support, who have made the decision to issue an RFP for the purpose of procuring a Next Generation 9-1-1 (NG9-1-1) system or some of those components. Specifically, this document recommends a structure and content to guide a project team that has been given the charter to develop an RFP. The guidance contained in this document assumes the proper procurement decisions have been made and resources to support the development of the RFP are secured.

The journey to NG9-1-1 is complex and consists of many factors that need to be considered during procurement, especially the impact on certain elements of Public Safety Answering Point (PSAP) operations. This list may include, but is not limited to, the following:

- Impact on stakeholders
- Impact on operations
- Impacts on technology
- Impacts on security and cybersecurity

It may be helpful to assist PSAPs in understanding how a transition to an NG9-1-1 system as a result of a procurement may impact their future purchasing decisions and budget in the areas mentioned above, as they may be dealing with a different procurement authority, budget cycle, and rules and regulations established by that authority. It is therefore incumbent upon 9-1-1 Authorities, their consultants, and PSAPs to make every effort to involve all impacted stakeholders in every step of a planned procurement.

This document attempts to describe an overview of the various steps necessary to research and develop an NG9-1-1-centric RFP. The many elements of the development of an NG9-1-1 RFP effort require consideration of the following:

- Reasons for issue or release
- Cost factors associated with the procurement of software, hardware, services, and maintenance
- RFP preparation and procurement rules
- Partnerships with other 9-1-1 authorities or agencies
- Decisions regarding the engagement of third-party subject matter experts
- Costs associated with preparation include the following:
    - Identifying personnel who may be part of the RFP development process, evaluation, and review activities
    - Analyzing the impact on their existing responsibilities
    - Reviewing their current schedule
    - Understanding the potential need for overtime
- Governance and regulatory issues

- Future organizational and staffing plans
- Data development issues
- NG9-1-1 system acquisition and migration options plans

While this document provides a comprehensive guide, using it as a standalone resource may overlook the unique resource list needs of procurement requirements of states, counties, and municipal jurisdictions.

This document will assist anyone involved in developing an RFP to procure elements of an NG9-1-1 system, including PSAP Functional Elements, NG9-1-1 Core Services, Geographic Information System (GIS) Data and Services, and Management Information System (MIS) Data Collection and Reporting.

Table of Contents

NENA
INFORMATION DOCUMENT
NOTICE

This Information Document (INF) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. It is not intended to provide complete design or operation specifications or parameters or to assure the quality of performance for systems that process such equipment or services.

NENA reserves the right to revise this Information Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for changes to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911

or crm@nena.org

2 Document Conventions

NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally-available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at https://www.nena.org.

2.1 NENA Intellectual Property Rights (IPR) and Antitrust Policy

NOTE – The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at https://www.nena.org/ipr.

Consistent with the NENA IPR and Antitrust Policy, available at https://www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement any standards referenced by this document or to implement or follow any recommended best practices, procedures, or architectures contained herein.

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911

or crm@nena.org

2.2 Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA-INF-021.1-2020	January 19, 2020	Initial Document
NENA-INF-021.2-2026	August 12, 2026	Add material to address advances in NG9-1-1 Standards.

3 Considerations for Procurement of NG9-1-1 System Elements

The following sections cover several dimensions of information that can be included in any procurement process such as a Request For Information (RFI), Request For Quote (RFQ), and/or an RFP. The focus of this document is primarily on RFPs.

The more complete each dimension of a proposal, the fewer assumptions vendors must make. This may increase the accuracy and reliability of the response.

The specific RFP consideration to be used by stakeholders procuring PSAP Functional Elements, NG9-1-1 Core Services, GIS Data and Services, and MIS Data Collection and Reporting are defined in the following subsections:

- Collaboration with Procurement Authorities (Section 3.1)
- Research (Section 3.2)
- Planning (Section 3.3) – Scope of Your Project/NG9-1-1 Transition Planning
- RFP Content Considerations (Section 3.5) – With additional scope provided via diagrams, tables, and checklists
- NG9-1-1 System Elements for Procurement (Section 3.7)
- RFP Drafting and Issuance (Section 4.1)
- Contract/Terms and Conditions (Section 4.4.3.12)
- RFP Response and Evaluation (Section 4.6)

3.1 Collaboration with Procurement Authorities

PSAPs that are under the auspices of procurement authorities should be mindful of rules and regulations established by those authorities, and should make every effort to involve them in every step of a planned procurement.

3.2 Research

Developing an RFP for procuring all or part of an NG9-1-1 system is only one part of the overall system procurement process. Prior to developing the RFP, one should take into consideration the need to research the desired system needs versus what is available. Research steps to consider in preparing for the release of an RFP could include the following:

- Conducting a basic online search for NG9-1-1
- Locating and reading industry-related articles and standards
- Attending industry events to meet others who may have NG9-1-1 procurement experience
- Attending industry events to find vendors providing NG9-1-1-related products and services
- Issuing an RFI to gather intelligence on currently available systems and services from vendors

3.3 Planning

A 9-1-1 Authority intending to migrate from a legacy Enhanced 9-1-1 (E9-1-1) system to an NG9-1-1 system should take the time to consider and address a number of issues. Specifically, 9-1-1 Authorities should consider developing the following seven plans:

1. Financial Plan—Costs and Funding
2. Governance Plan
3. Federal and State Regulatory Plan
4. Organizational and Staffing Plan
5. Data Development Plan to Support an NG9-1-1 System
6. NG9-1-1 System Acquisition Plan
7. Migration Plan

3.3.1 Financial Plan—Costs and Funding

The financial planning process is a critical step 9-1-1 authorities should take when developing a multi-year budget needed to deploy NG9-1-1 network systems. Considerations should include the following:

- How much it will cost to migrate to NG9-1-1. This should include non-recurring and recurring costs, capital expenses, and operating expenses.
- The ongoing costs once the system is in production.
- The forecasted funds to be collected, which can potentially be applied to the NG9-1-1 system.
- Other sources of funds that may be available to the 9-1-1 Authority to support the migration. For example, many states provide grant funding to 9-1-1 Authorities that can be used to support the migration to NG9-1-1. In addition, at the time accepted industry best practices were being updated elsewhere, the Federal Government is considering a bill, the Spectrum Auction Reauthorization Act of 2023 [2], tied to the auction of spectrum, that could make up to $15 billion available in a grant program. If this bill is passed, these funds would be available to the states to help fund the migration to NG9-1-1.
- A plan for peak spending while both the E9-1-1 and NG9-1-1 systems are running in parallel.
- Plans using federal or state funding may have terms and conditions tied to the use of the disbursement.

3.3.2 Governance Plan

The governance planning process is the step 9-1-1 Authorities should consider taking to develop how the NG9-1-1 system will be managed and used to guide its future activities. Governance models developed may include the following:

- Identification of the group that will have the authority, knowledge, and commitment to make decisions about the migration to NG9-1-1.
- Identification of the body that will oversee the NG9-1-1 system when it is in production.
- The method of interaction between the project team and governing body, including project team authority levels for changes and identification of the change process.

3.3.3 Federal and State Regulatory Plan

The federal and state regulatory planning process is the step 9-1-1 Authorities should consider taking to identify the various levels of regulation and mandates of the NG9-1-1 system to guide its future activities.

Federal and state regulatory models developed may include the following:

- Federal and State reporting requirements
- Current rules that support the anticipated migration

3.3.4 Organizational and Staffing Plan

9-1-1 Authorities should use the organizational and staffing planning process to develop how the organization as a whole, and the associated staff, can be structured to guide its future activities. Organizational and staffing models developed may include the following:

- Identification of existing staff levels and their various roles.
- Identification of roles specific to data rights management.
- Identification of staffing requirements during the migration process, with consideration given to required roles and skills during and after each migration phase.
- Evaluation of post-migration staffing requirements as new roles and staff may be needed.
- Reconsideration of organizational structure and management in light of the potential changes.
- Consideration to the use of consultants to augment, on a temporary or permanent basis, the necessary skills and staffing requirements.
- Special consideration to the responsibility for Cybersecurity in the organization.

3.3.5 Data Development Plan to Support an NG9-1-1 System

The data development planning process is the step 9-1-1 Authorities should consider taking to develop how the NG9-1-1 system and the necessary data will be managed and used to guide its future activities. Data development models developed may include:

- The data required to support an NG9-1-1 system (Emergency Call Routing Function [ECRF], Location Validation Function [LVF], Mapping Data Service [MDS], MSAG Conversion Service [MCS], Geocode Service, Service/Agency Locator, and, if

applicable, the Location Information Server [LIS]) and Additional Data Repository must be available and of a satisfactory quality.
- Assurance that GIS information is available, and processes are in place to maintain the accuracy and quality of the data in a timely manner.

3.3.6 NG9-1-1 System Acquisition Plan

The system acquisition planning process is the step 9-1-1 Authorities should consider taking to develop how the NG9-1-1 system should be procured, ordered, and implemented and used to guide its future activities. Acquisition models developed may include the following:

- Definition of system requirements, and the needs and requirements of participating groups that may have to be addressed.
- Identification of system elements that are deemed "essential" versus those elements that are considered to be "optional."
- Determination of the implementation timeline, after determining the desired system architecture and design.

3.3.7 Migration Plan

The migration planning process is the step 9-1-1 Authorities should consider taking to develop how the NG9-1-1 system will be placed into operation and used to guide its future activities. Migration is discussed in *NENA NG9-1-1 Transition Plan Considerations Information Document*, NENA-INF-008 [3].[1]

Migration plan models developed may include the following:

- Defining the NG9-1-1 system to replace the existing E9-1-1 system.
    - The topics above, if covered properly, should provide the necessary level of definition and set expectations with vendors during the procurement process.
- Defining how the migration to the NG9-1-1 system will be achieved.
    - 9-1-1 Authorities should make vendors and service providers aware of their expectations and note any limitations of which the vendors should be aware.
    - Information on migration to NG9-1-1 can be found in NENA-INF-008 [3].

3.3.8 Planning Summary

The seven plans listed above are interrelated. Decisions or limitations in one plan will impact options in other plans. Development of each plan can occur somewhat independently of all other plans; however, there are interdependencies that require decisions to be made in some plans before work on other plans can progress.

[1] Some information in the NENA-INF-008 [3] document may be outdated for some implementations, but it raises many issues that must be considered in any transition to NG9-1-1. There is no newer document.

For example, the investment in time and money to develop an RFP should not be made until the 9-1-1 Authority has a reasonable expectation that it can afford to move forward with the migration. Since the costs of staffing the project and developing the underlying data should be included in the Financial Plan, some work in these areas is also required.

Some plans are subject to scheduling limitations. For example, changing state statutes and regulations that affect the migration to NG9-1-1 can be impacted by the state legislative calendar. Missing deadlines in the legislation process can create significant delays. The timing of RFP development should take into consideration the status of all other plans.

3.4 Value of Standards

As with E9-1-1, Next Generation 9-1-1 is defined by standards—documents created by a consensus driven process with all stakeholders that multiple vendors can implement such that they all interoperate. Standards are vital to the success of NG9-1-1, and conformance to standards brings many benefits to 9-1-1 Authorities, responders, and the public. While standards have been developed by a number of Standards Development Organizations (SDOs), the primary foundational standard ***was*** developed by the NENA Development Group. The "i3" standard, *NENA i3 Standard for Next Generation 9-1-1*, NENA-STA-010 [4], embraces standards developed by other SDOs, and standards developed by other SDOs have been developed to complement the i3 standard, most notably, the SIP standards developed by the Internet Engineering Task Force (IETF). Every RFP issued in North America for NG9-1-1 has specified the i3 standard.

Purchasers have a choice of vendors because standardized components selected from different vendors will reliably work together. Different vendors can't represent that their products are fully interoperable with each other unless 1) they commit to meeting standards, 2) they have done interoperability testing, and 3) they are willing to document their actions in doing both. Note that, "meeting standards" requires specifying which standards, and that response phrases such as 'equivalent to' or 'consistent with' may mean that the product doesn't meet the literal standard, but is what the vendor feels is 'good enough' (for now) and is economical for them to build and sell, or is their view of 'what you really need'. This will invariably lead to upgrades to handle new developments and new charges. Failing to deal with these issues fully will jeopardize interoperability.

Reliability is higher because the standards are written to require modern redundancy and reliability features, and the system architecture has had wide review by a large number of skilled practitioners which assures purchasers that no significant architectural flaws exist.

In disaster and significant failure scenarios, calls can be handled by any available service because they all work the same way, driven by the same standards.

All NG9-1-1 RFPs should require conformance to the appropriate standards, most importantly, NENA-STA-010 [4] , the current i3 standard. Proposers must be encouraged to implement the standards faithfully. Where there are extenuating circumstances, proposers

should be required to state where they don't meet any aspect of the standard, state a satisfactory reason why, specify when they will achieve conformance, and detail the penalty they propose for not meeting the proposed dates. The penalty for knowingly misstating conformance should be severe, but because the standards are complex and large, accidental non-conformance should not be handled the same way, and vendors should be given a reasonable time (measured in months, typically 6-9) to update their system to be compliant.

NENA standards define a set of Functional Elements (FEs), which are groupings of functions, where the interfaces between FEs are carefully described. The intention of the standards is that an FE from one vendor be interchangeable with the same FE from another vendor, and a complete NG9-1-1 system be able to be assembled from a set of FEs from multiple vendors which works in every respect.

The standards also state that it is not a requirement that an FE be built as a stand-alone system or self-contained implementation. Rather, any set of FEs may be combined into a single system or implementation, provided that the set implements all of the functions the standards define for the set and the interfaces to the combined set provide all of the external interfaces to the set. If the standard defines an interface between two FEs, and an implementation combines the FEs into one system, the interface between the two FEs inside the system doesn't have to use the specified interface; those FEs they can use anything the vendor wishes to use. If a system incorporates multiple FEs, it may use proprietary interfaces between them internally, as long as it supports the standard interfaces for external elements from other vendors. Vendors should be free to group FEs as they see fit, so long as the set in a physical implementation has all of the external interfaces and combined functions defined for the set.

To assist with conformance to the applicable standards, several voluntary programs have been or will be established. For example, NENA conducts a series of Industry Collaboration Events (ICE) [5] which affords vendors the opportunity to test their implementations against other vendors' implementations of the various NG9-1-1 Functional Elements. Participation is strictly voluntary, and the rules of ICE require that no participant reveals any information, including results, of any other participant. Participants are free to disclose anything they want about their own experience, so long as it does not reveal any information about any other participant. RFPs may wish to enquire whether a proposer participated in ICE, and what their results were, keeping the above non-disclosure requirements in mind. More information about the NENA ICE program can be found at https://www.nena.org/page/ng911_ice [5].

To provide 9-1-1 Authorities an unbiased assessment of FEs provided by vendors, at the time of development of this document, a new, complementary program is under development: the NG9-1-1 Interoperability Task Force. This voluntary program intends to provide an unbiased testing lab that will assess conformance of FEs to established industry

standards. Participation in the program and results of these tests will be available to 9-1-1 Authorities and should be used in developing an RFP and evaluating vendors' responses. In addition to testing conformance of individual FEs to the standards, the program will also test interoperability between FEs provided by vendors and, ultimately, end-to-end testing. More information about the NG9-1-1 Interoperability Task Force can be found at https://ng911interop.org/ [6].

Standards evolve, and the current iteration of NENA-STA-010 [4] is continually being reviewed for updating, as determined by the evolution of this industry. Vendors can't control what the next version will contain, but if they participate in standards activities, they can have a voice, and also know in advance what changes a new version will bring. It is highly desirable that NG9-1-1 deployments keep up with the standards as they evolve. By the same token, vendors are reluctant to actually start modifying their products until they are sure they know what the new standards will say, and thus there is always a considerable time lag from when a new version of a standard or the initial version of a new standard is released, and implementations of that version are released. The RFP should discuss this issue. It is suggested that proposers be required to implement new versions and that the proposal state the timeline for such upgrades. Customer flexibility is key here, because a new version may require a vendor to make a significant change to its architecture that can take a longer time to complete. Although standards writers are sensitive to the effect of changes to existing implementations, the fact is that standards evolve, and implementations must evolve with them.

Vendors often go beyond standards, adding proprietary features to their products to make them more attractive to customers. The challenge for customers is that these features engender vendor lock-in. A careful consideration of such extensions should be made in evaluating proposals so that the Authority understands what vendor lock-in they have to contend with, how comfortable they are with that, and what they might do if, for some reason, a vendor change was needed. Clearly, being able to take advantage of features without being dependent on them is desirable. Proposers should be required to make such extensions backward compatible—meeting the standards without reservation, and capable of interworking with other implementations that don't have the extensions. NENA standards are designed to be extended, so that new versions can be deployed incrementally with older implementations continuing to work while newer implementations are deployed. These same extension points can be used by vendors to achieve backwards compatibility with other standards-based implementations. Proposals that require proprietary extensions to provide functionality described by the standards should not be permitted.

3.5 RFP Content Considerations

To solicit a clear response to the RFP, the writer must articulate the scope of the 9-1-1 Authority's requirements from an operational and policy management level to the vendor community. This articulation should establish clear points of demarcation for the vendor for

what the 9-1-1 Authority's vision of enabling NG9-1-1 capabilities is, in what areas the 9-1-1 Authority is seeking to gain insight, or technical solutions and which areas are seen as being retained by the 9-1-1 Authority for technical operation. It is vital that the RFP writer address the end-to-end scope of the requirements to ensure that "gaps" that might exist between parties involved in providing NG9-1-1 components of the procured solution and their relationship to the 9-1-1 Authority-owned or -operated components are managed. "Gaps" in responsibility along the NG9-1-1 solution "call chain" and data chain should be actively addressed in the procurement process to eliminate single points of failure introduced by incomplete reviews of responsibilities in the acquisition process.

The scope identified by the 9-1-1 Authority should clearly establish the range of the services on which the 9-1-1 Authority is seeking information or seeking technical assistance or solutions with regard to the Emergency Services Internet Protocol (IP) network (ESInet), NG9-1-1 Core Services, and NG9-1-1 GIS data preparation activities. For the ESInet and NG9-1-1 Core Services, the RFP writer's decision on which solutions will be provided via a Hosted Solution, Managed Solution, or Cloud Solution, and which will be provided through an in-house owner-operated model, will influence the type of RFP requirements for the specifications. Likewise, the RFP writer may be seeking consultative assistance across the spectrum of NG9-1-1 solution components.

3.6 Host, Manage, and Cloud Explained

3.6.1 Hosted Solution

- Host: A system that can be located on premises and off at two different PSAP/ECC locations for diversity. Hosting is maintained by the host or hosts for the main Nodes. Side A and Side B Node can be located separately.
- Host Remote sites, Remote workers: Can connect to this configuration.

3.6.2 Managed Solution

- Managed: Another party maintains and services a solution regardless of where it resides.
- Managed: Connection by Network to a location off premises, such as a data center or Central Office.
- Managed Remote sites, Remote workers: Can connect to this single or multitenant configuration.

3.6.3 Cloud Solution

- Cloud: Virtual servers are located and accessed on an IP Cloud Network.
- Cloud Software as a Solution (SaaS): Access by desktop software to core servers that are fully virtual and maintained by a Network Cloud provider. SaaS is all about delivering a software service through the network connection to a cloud provider, or

a desktop is being used to just connect to a web browser portal, and the core servers deliver calls to a cloud environment and then down the network to the PSAP/ECC. Software solutions are all in the cloud.

- Cloud based PSAPs/ECCs fall under one of the following configurations: a Remote, a Host Remote site, a Remote worker, or a multitenant configuration. Single tenant configuration can be costly for a small PSAP/ECC.

As an aid in managing clarity of the scope for the RFP writer, this section provides several contextual visual planning aids in the figures and tables below. Other sections of this document provide more detailed explanations that relate to the elements contained in the contextual visual aids.

3.6.4 Logical Overview

Figure 3-1 Logical Overview of an NG9-1-1 System below provides a high-level end-to-end overview of an NG9-1-1 System, from the originating network to the PSAP. Figure 3-1 depicts the ESInet (discussed in Section 3.7.1), Geographic Information Systems (discussed in Section 3.7.2), Next Generation 9-1-1 Core Services (discussed in Section 3.7.3), NG9-1-1 PSAP/ECC Functional Elements (discussed in Section 3.7.4), and Management Information Systems (discussed in Section 3.7.5). A more detailed and technical diagram may be found in NENA-STA-010 [4].

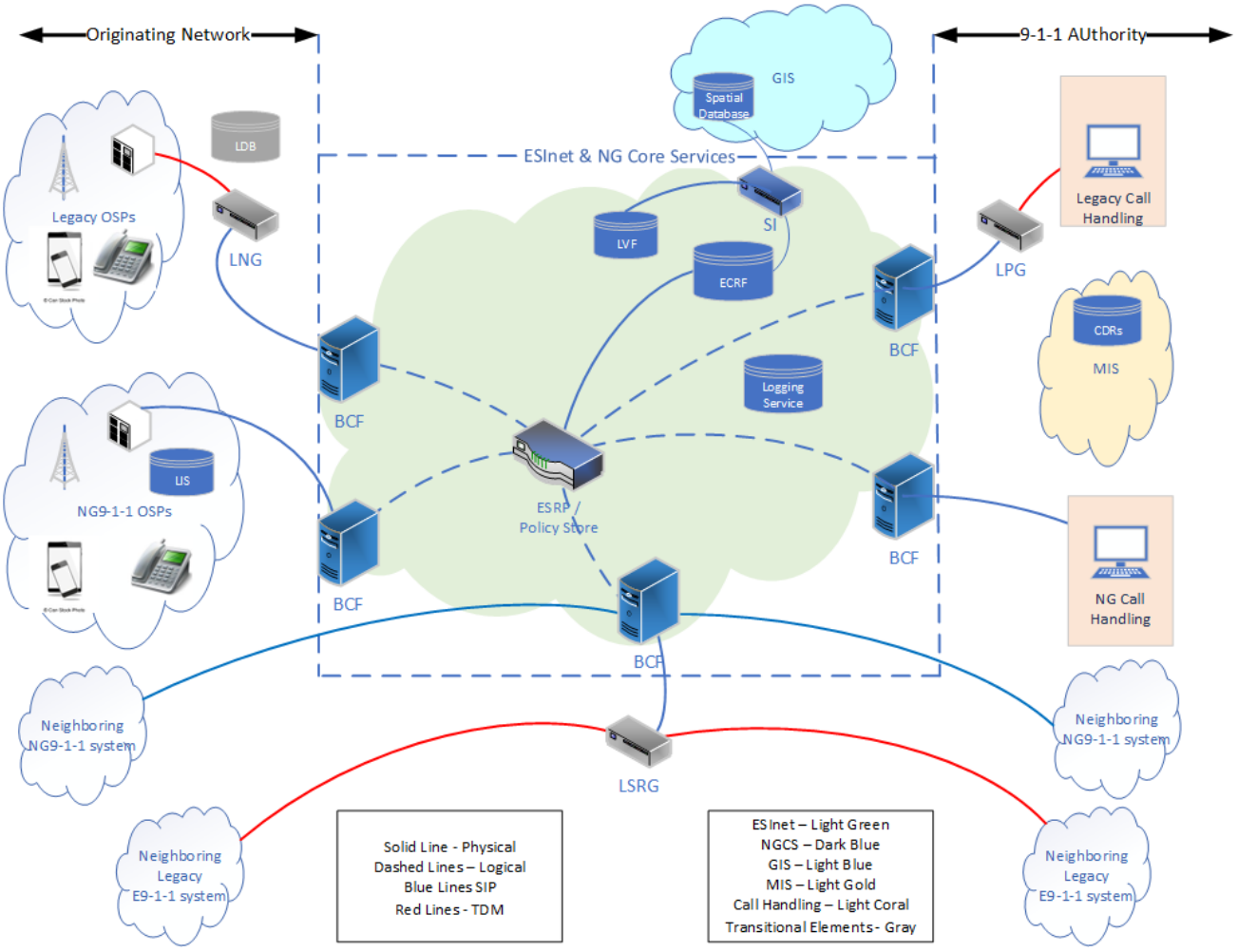

Figure 3-1 Logical Overview of an NG9-1-1 System

Table 3-1 RFP Scope and Responsible Party Matrix Worksheet below is provided as a planning worksheet for the RFP writer to place an 'X' in the appropriate spaces within the matrix according to the anticipated strategy.

Having completed the matrix, it is strongly recommended that the RFP writer include a Topology Diagram in the RFP to visually convey the overall vision for the NG9-1-1 effort associated with the RFP, clearly indicating which components are existing, which are in the scope of the RFP, and which might be in the scope of future projects or other authorities.

Table 3-1 RFP Scope and Responsible Party Matrix Worksheet

NG9-1-1 Component			State		Regional		County/PSAP		Agreements			Working Notes
Group		Sub-Components	Hosted	In-House	Hosted	In-House	Hosted	In-House	Service Level	Consulting	Interconnect	
ESInet Domains	Network Infrastructure	Wide Area Network (WAN)										
		PSAP Local Area Network										
	Network Management	Network Operations Center (NOC) Managed Services										
	Firewall	Border Control Function (BCF)										
	Edge Gateways & Transition Elements	Legacy Network Gateway (LNG)										
		Legacy Selective Router Gateway (LSRG)										
		Legacy PSAP Gateway (LPG)										
		Location Database (LDB)										
NG9-1-1-= Core Services	Functional Interfaces	Emergency Service Routing Proxy (ESRP) (Originating and Terminating)										
		Policy Routing Function (PRF)										
		Emergency Call Routing Function (ECRF)										
		Location Validation Function (LVF)										
		Alert/Alarm Management										
		Logging Service										
		Log Event Replicator										
		Time Server										
		Spatial Interface (SI)										
		Mgmt. Info System										
PSAP Functions		Call Handling FE										
		Collaboration FE										
		Incident Handling FE										
		Dispatch FE										
		Logging Service										
		LogEvent Replicator										
		Mgmt. Info System FE										
		Time Server										
		Management Console FE										
		Alert/Alarm Management										
		Interactive Media FE										

3.7 NG9-1-1 System Elements for Procurement

Due to limitations in time, funding, and authority, parts of a complete NG9-1-1 system may be procured and implemented in phases or by different entities. Accordingly, an individual RFI/RFP may focus on acquiring one or more components among those that comprise an NG9-1-1 system.

Readers are encouraged to thoroughly review the section or sections covering the components of an NG9-1-1 system that will be included in the RFI/RFP. However, readers should also review sections that are applicable to all NG9-1-1 system components, including HMI (Section 3.8), Transitional FEs and Services (Section 3.9), SLAs (Section 3.10), Security & Cybersecurity (Section 3.11), and References (Section 7).

3.7.1 ESInet (IP Transport Infrastructure)

RFPs seeking an ESInet should incorporate the provisions contained in this section of this document.

3.7.1.1 Introduction

Guidance for this section has been taken from the *NENA Emergency Services IP Network Design (ESIND) Information Document*, NENA-INF-016 [7]. ESInets are private, managed IP networks. An ESInet serves a set of PSAPs, a region, a state, or a set of states. ESInets are interconnected to neighboring ESInets so that traffic can be routed from any point in the ESInet to any point in any other ESInet.

The ESInet is fundamentally a collection of IP circuits and routers that forms the network that connects the PSAPs.

The ESInet is defined in the NENA Knowledge Base Glossary [1] as follows:

> *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 NGCS (Next Generation 9-1-1 Core Services).*

3.7.1.2 Background Information

Many ESInets have been or are being built as 9-1-1 entities prepare to migrate to NG9-1-1. The ESInet is a network of IP networks that connects the various 9-1-1 entities that are to be included.

ESInets are like other IP networks in that they are a collection of routers and links between routers, in which there are multiple paths, such that link failures leave at least one link path usable by the network. ESInets, however, must be designed to meet more stringent requirements for security and reliability service levels than most other IP networks.

Details on ESInet characteristics can be found in NENA-INF-016 [7]. Below is a summary of the requirements for an ESInet for NG9-1-1 Core Services:

1. The network between the PSAP and the ESInet will be private or a virtual private network (VPN) that supports, at a minimum, Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), and Real Time Protocol (RTP).
2. It will have scalable bandwidth to support new enhanced services. Some existing network infrastructure, like a legacy Frame Relay network, is not scalable enough for an ESInet and may present other problems. Other legacy technologies like Asynchronous Transfer Mode (ATM) are scalable, but present other issues. Metro Ethernet or Multi-Protocol Label Switching (MPLS) are preferred over ATM for this reason. NENA-INF-016 [7] describes multiple options to choose from for building ESInets that support scalable bandwidth and provides details on other advantages and disadvantages for each option. All of this should be considered when developing the requirements for an RFP to procure ESInet infrastructure and NG9-1-1 Core Services.
3. The ESInet shall be a conventional routed IP network.
4. Multiprotocol label switching (MPLS) or other sub-IP mechanisms are permitted as appropriate.
5. How PSAPs will connect to the ESInet should be considered in the procurement process. Where possible, PSAPs should have redundant connections to the ESInet.
6. The PSAP's LAN and connection to the ESInet must be resilient, secure, physically diverse, and logically separate.
7. The ESInet shall be engineered to sustain real-time traffic, including data, audio, and video.
8. Connections between the PSAP and ESInet shall support TCP/IP connections with Transport Layer Security per NENA-STA-010 [4].
9. All components of the ESInet and any elements connected to it must support both IPv4 and IPv6. New deployments must use IPv6.

3.7.1.3 Interdependencies with Other NG9-1-1 Components

3.7.1.3.1 Other NG9-1-1 Components that Must be Implemented Prior to or in Conjunction with ESInets

The ESInet and NG9-1-1 Core Services are both required elements for an NG9-1-1 system. The NGSC provides the call routing intelligence and many other functions in an NG9-1-1 system. See NENA-STA-010 [4] for information on NG9-1-1 Core Services (NGCS).

ESInets connect to the Internet, to other ESInets, and to PSAPs.

- Originating Network Interface: The ESInet connects directly to local Origination Networks via private connection, and also accepts calls from any origination network or device from the Internet. All calls, regardless of origin, including calls from legacy origination networks via a Legacy Network Gateway (LNG) or Legacy Selective Router Gateway (LSRG), pass through a Border Control Function (BCF) before connection to any other NGCS function. The calls are presented to the Emergency Services Routing Proxy (ESRP) in the right ESInet as directed by the Emergency Call Routing Function (ECRF). The ESRP then routes the calls within the ESInet towards the right PSAP.
- PSAP Interface: The NG9-1-1 PSAP call interface is a SIP call interface. The ESRP routes calls towards the right PSAP. In each ESRP, the PRF is used to interpret the current route policy of the next hop based on the state of the downstream entity. The terminating ESRP routes to a PSAP. Calls are presented to a legacy PSAP through a Legacy PSAP Gateway (LPG).
- Border Control Function: A BCF sits between external networks and the ESInet and between the ESInet and agency networks. All call traffic from external networks, LNGs, and LSRGs transits a BCF, which provides security for downstream call processing elements.

See Section 3.7.3 NG9-1-1 Core Services (NGCS) for details on these components.

3.7.1.4 Information to Provide Proposers about ESInet

It is recommended that the information below be provided to proposers in an RFP for ESInet and NG9-1-1 Core Services.

1. Any existing or planned network facilities available to the jurisdiction need to be identified. Sharing of the ESInet with other network facilities is encouraged, in order to save cost, provided that the NG9-1-1 traffic can properly co-exist with existing traffic and will be assigned the appropriate traffic priority markings.
    a. Network facility stakeholders associated with existing network facilities need to be identified. This includes the provider of the existing facilities and current users of the facilities.

b. The timing of their availability needs to be identified. Are the network facilities available now or at some point in the future?

c. Any other traffic that the network is carrying will need to be identified. Facilities will need to be sized appropriately to accommodate the different types of traffic that are on the network. Appropriate segregation of other traffic so that it does not interfere with NG9-1-1 traffic is required. If the ESInet shares an IP network topology with other traffic, the other traffic may need to be conditioned using *An Architecture for Differentiated Services*, RFC 2475 [8] (DiffServ), so that NG9-1-1 traffic has appropriate priority.

d. The capacity of the network facilities will need to be identified. Existing facilities may exist but require augmentation before they can be used for public safety purposes.

e. Security associated with the existing facilities will need to be assessed. Entities that currently have access will need to be identified, and security measures associated with their access will need to be reviewed.

f. Network management and trouble ticketing capabilities of the network facilities will need to be identified.

2. The scope of the ESInet and NG9-1-1 Core Services needs to be provided to proposers of ESInet services. This should state whether the ESInet and NG9-1-1 Core Services will be statewide or regional, and include the addresses of the PSAPs and data centers that are to be included. Location of likely interconnect points with origination networks should be identified. Likely interconnection points with neighboring ESInets should be identified. If the physical location of the data center(s) matters to your deployment, consider making that very clear, as it could affect the number of potential suppliers, as well as the cost of the system.

3. The extent of the ESInet and NG9-1-1 Core Services should also be described. This should include the point(s) of ingress and egress to the ESInet.

   a. Any specifically desired ESInet topology should be described in detail, with understandable logical diagrams. If proposers are to propose a topology, any requirements of the agency should be provided. Proposers should be required to provide clear diagrams. Diagrams and descriptions should clearly define points of ingress to the ESInet. For this document, the point(s) of ingress will be referred to as points of interconnection or POIs.

   b. It may be necessary to consult with your OSPs, NGCS provider, and the governing regulatory framework for the location of POIs related to the necessity or preferences of them being physically located in state or if they

can be out of state. In some cases, there may be restrictions against routing 9-1-1 calls to an out-of-state POI.

i. The FCC NG9-1-1 transition phase 1 and phase 2 rules do detail this consideration as a requirement for making a valid request.[2]

c. All points of egress from the ESInet should be clear in all diagrams and descriptions. These may include interconnections to PSAPs, other ESInets, and redundant instances of the ESInet.

d. How the proposed ESInet will support the NG9-1-1 Core Services it will host should be clearly shown and stated. Geo-diverse redundancy is a requirement for the ESInet (and the Core Services it hosts). Any specific requirements should be clearly stated. Proposers should describe how their ESInet redundancy scheme will meet the availability requirements for NG9-1-1 deployments.

e. Interconnection with all external networks should be clearly described and depicted on any diagrams. These would include networks that host supporting services and functions outside of the 9-1-1 Authority's control.

4. Clearly describe the required bandwidth parameters.

   a. The ESIND document contains some heuristics tied to call taker positions and PSAPs. State clear requirements on how bandwidth is affected by network failures. For example, if there are three redundant connections between two points in the network, does the bandwidth requirement have to be maintained if one or two connections fail?

5. Clearly describe the redundancy requirements.

   a. Explain requirements for redundant facilities where it is important to specify directly (as opposed to specifying reliability requirements and allowing proposers to determine redundancy needed to achieve the reliability which may be preferred). State the requirements for what capacity/capability must be maintained when one (or more) redundant paths fail.

6. State the Border Gateway Protocol (BGP) requirements.

   a. If the ESInet is required to use Border Gateway Protocol, state clearly if it must be configured and managed as an Autonomous System (AS). If there are requirements for a particular interior gateway protocol, state them. Describe what options PSAPs must have to connect to the ESInet at the protocol level.

[2] 47 CFR 9.31(a)(4) (2024)

7. Explain requirements/options for using shared facilities.
    a. State whether proposers can/should share facilities with other networks/network components, and/or what network segments or facilities must be exclusive to the ESInet to be acquired. Where sharing is allowed (which is generally to be encouraged), state what isolation is required between users to maintain the appropriate level of service the ESInet requires. Interconnection is accomplished by negotiated interconnection agreements between the parties making the connection, such as the Originating Service Provider and the entity owning/operating the NG9-1-1 network, or a provider of network resources for other purposes. It is prudent for the 9-1-1 Authority or equivalent to get a commitment on time-to-accomplish up front, along with the agreement on exactly what is to be provided and accomplished. There are no standards for this process, as it is a negotiated business agreement.
8. Explain requirements/options for Public Addressing.
    a. State how much public address space (IPv4 and IPv6) must be made available to the ESInet or provide sufficient information so a proposer can calculate how much space will be needed. Note that NENA-STA-010 [4] requires all new implementations to use IPv6. Consider future needs, as renumbering addresses is difficult. State whether NAT is allowed (ESIND suggests not).
9. State clear requirements for security.
    a. Consider requirements for secure versions of routing protocols. State any requirements for the physical security of key network elements. State requirements for what security proposers must meet for admin/network operations access to network elements, both in terms of requirements on devices and operational security for the proposer and 9-1-1 Authority staff. Both physical security and cybersecurity merit full focus and attention for Public Safety systems. There are numerous references for physical security and a growing number of recommendations for cybersecurity, such as the *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*, NENA-STA-040 [9], *NENA Security Audit Checklist*, NENA-REF-012 [10], National Institute of Standards and Technology (NIST) material [11], Center for Internet Security (CIS) [12], and Department of Homeland Security (DHS) [13] requirements.
10. State the requirements for Network Management and Monitoring.
    a. ESIND contains specific guidance for network management and monitoring. Consider requirements for what level of access to network monitoring the NG9-1-1 Authority/PSAP staff should have. State what processes for

notification of network outages or degradation are required. Consider requiring redundant Network Operations Centers (NOCs). State what control the primary proposer must have over subcontractors providing network facilities to avoid circular finger-pointing.

11. Specify the Performance and Quality of Service Requirements.
    a. Specify the parameters required for packet loss, jitter and latency metrics, and where such requirements must be maintained (such as all paths emergency call media traverses). State Quality of Service (QoS) requirements and how they must be measured. Note the requirements in NENA-STA-010 [4] to support DiffServ. ESIND contains specific recommendations for traffic management. Consider which of those performance requirements should be specified in the RFP.

3.7.1.5 Information to Request from Proposers about ESInet

3.7.1.5.1 High-level ESInet Requirements

1. General Requirements for the ESInet

FCC Rules: Require proposers to address the appropriate rules that might apply, such as, but not limited to Part 15 of Title 47 of the Code of Federal Regulations dealing with Class A requirements for electromagnetic interference [14], and Part 12 of Title 47 of the Code of Federal Regulations dealing with Resiliency, Redundancy, and Reliability of Communications [15].

    a. ESInet Design Requirements: Require proposers to explain how their proposed ESInet solution follows or deviates from the guidelines provided in NENA-INF-016 [7], or its successor document.
    b. Facilitating Carrier Transition of Services to the ESInet: Require proposers to establish the need to transition existing 9-1-1 services from current service providers onto the ESInet and the terms and conditions between the proposed solution and the interfaces to the Originating Service Provider (OSP) and their terms and conditions.

2. ESInet Protocol Network Requirements
    a. Require proposers to describe how they support BOTH IPv4 and IPv6.
    b. Require proposers to describe what routing protocols are used in the network and where, how address numbers (both IP addresses and Autonomous System Numbers) are acquired and managed.

3. ESInet and NG9-1-1 Core Services Functional Transport Purpose Statement

a. Require proposers to state how their proposal supports all NG9-1-1 applications for voice and data. Require proposals to specify specific bandwidth for all links and show how the proposed bandwidth is sufficient to support voice, video, and text communications, and logging of the same. Require proposers to describe in detail how they maintain QoS. Request details of what Differentiated Services Code Points (DSCPs) will be used, what Per Hop Behaviors will be configured into each router for these DSCPs, and how policing of DSCPs will be accomplished at the interconnect points with other networks. Require a detailed analysis of how expected traffic will maintain the desired QoS and what network impairments would endanger maintaining QoS.

4. ESInet Interconnections Topology of Host and Remote Sites
    a. Require proposers to describe the topology of their proposed ESInet. Require a description of what routers will be provided, where all links to each router are connected to, what technology each link uses, and the bandwidth provisioned on it at network acceptance as well as what provisions are made for increasing bandwidth as the network grows. Require specification of interconnects between origination networks and other ESInets: location, technology, and link capacity. By graphical depiction or reference to a supporting appendix, provide the contextual inventory of the host and remote sites that are part of the procurement which proposers can use as an input to design of an appropriate network solution using the anticipated call volume and network bandwidth available.
5. Bandwidth Growth
    a. Require proposers to specify how their proposed ESInet can grow in a managed, incremental process over the expected lifetime of the contract and beyond it.
6. Real-time Application Monitoring
    a. Require proposers to describe real-time application monitoring functionality.
7. ESInet Architecture Guidance and Requirements (detailed in NENA-INF-016.2)
    a. Assess the availability of local IP networks.
8. Scalability – Expansion Requirements
    a. Require proposers to describe how the network can scale to meet anticipated and unanticipated new requirements, require descriptions of what expansion is possible by upgrade, and what requires replacement, what costs are involved, and what lead times are anticipated.

9. Network Upgrades and Maintenance
    a. Articulate the notification period for when downtime is required (e.g., five business days in advance) and the standard operating procedure (SOP) that describes the procedures agreed to in advance to mitigate the impacts of maintenance.
    b. Include a requirement to obtain the provider's Continuity of Operations plan.
10. Bandwidth
    a. Specify the current number of 9-1-1 Trunks, Admin Lines, and anticipated call volume for each PSAP that is part of the ESInet. Indicate the PSAPs currently handling or planning to handle calls at another PSAP for "x" period of time. RFP authors would need to provide an initial forecast of growth expectations, based upon the growth of not only voice, but video and other media types.
11. ESInet Availability
    a. Specify the availability requirement for the ESInet. ESInets that host NG9-1-1 Core Services always have a "five nines" availability requirement, that is, 99.999% uptime. Individual PSAP connection infrastructure may have a lower availability requirement in cases where NG9-1-1 routing features like call diversion are employed to provide an overall 9-1-1 service availability of 99.999%. State your requirements clearly and require respondents to describe how their solution will achieve the required level of availability, including a complete description of how redundancy and geodiversity are employed in the proposed design.
    b. Proposers should state their expected Mean Time To Repair (MTTR) for possible failures. RFPs should provide examples of potential failures.
    c. Proposers should require respondents to "show your work" and update the MTTR calculation when actual failures occur. Also, direct respondents to the *NENA NG9-1-1 Operational Diversity and Redundancy Information Document*, NENA-INF-047 [16] for details.
12. Network Facility Interfaces
    a. Require clear identification of where all interconnect points for origination networks are physically located, and the role of each interconnect point in the redundancy scheme being proposed. Require proposers to explain how the overall scheme will meet the specified availability requirements.
13. Network Monitoring
    a. Specify the requirement for monitoring the ESInet transport structure on a 24-hour-a-day, 7-day-a-week, 365-day-a-year basis and what protocols will be

required (e.g., Simple Network Management Protocol Version 3 [SNMPv3], Network Configuration Protocol [NETCONF], or other available protocols).

b. Describe how the proposed solution provides logs of network problems, including portal access and ad-hoc query features. The RFP should also specify a requirement for information on log retention.

c. Require proposers to describe in detail operations of the Network Operations Center (NOC) and staffing requirements for restoration or mitigation of incidents that are encountered.

d. Introduce requirements for a trouble ticket system and require proposers to describe how such information is presented to the jurisdiction, the severity and classification of the issues, and how issues are prioritized, tracked, and managed until trouble ticket closure.

14. Managed Network Services

a. Require proposers to describe their approach and processes for Managed Network Services (MNS) to perform operating system updates, anti-virus software used, security software, disaster recovery, applications software status, and any outsourced MNS services and methods of access for the jurisdiction to monitor equipment.

15. Cybersecurity Monitoring and Management

a. Request adherence to and knowledge of implementing cybersecurity monitoring and management for security monitoring and management in accordance with *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*, NENA-STA-040 [9], and other relevant NENA standards to address access control, user monitoring, security techniques and protocols, physical port protection, interconnections with other networks, other network qualifications, intrusion detection, and security event logging.

b. Have proposers describe their Security Operations Center (SOC) facilities.

16. Other Equipment Environment Considerations

a. An ESInet that hosts NGCS has physical, environmental, and security requirements similar to any critical infrastructure datacenter. Make certain that the RFP states the requirements clearly and have proposers explain how their solution will meet the requirements.

17. Current and New Equipment

a. Identify if there are allowances for trading in used equipment in the solution.

b. The use of out-of-date ESInet equipment should be avoided.

3.7.1.6 How to Evaluate Responses to ESInet RFPs

9-1-1 Authorities need expertise, which will often be through consulting arrangements, to rigorously evaluate the ESInet portions of a proposal. The expert needs to have significant design/implementation expertise in highly-available IP network design. Some general advice is below, keeping in mind that an ESInet is comprised of a set of routers and links, as well as the services that operate the routers and maintain the links.

1. Value diversity over quality. The most reliable networks have the most paths between endpoints. It's certainly true that the reliability of the network is proportional to the reliability of the links, so that if you are comparing two network designs that have the same link paths, but one proposal has more reliable links than the other, the more reliable link proposal would be favored. Increasing the number of paths has a greater influence on reliability than the range of reliability for typical links available for ESInets.
2. Favor actual geographic diversity. Ideally, all links going into a given facility would have entirely separate physical topology so that, for example, an excavator can't take out more than one link per incident.
3. An ESInet is a critical network – everything in NG9-1-1 depends upon it. Having only two ingress or egress paths to your ESInet is a minimum, and not really sufficient. In an IP network, ten paths are not too many. The network will route packets over any available path. Five nines of availability are needed for an ESInet, end-to-end, and different types of facilities so that if one type is knocked out, another will survive. Be realistic in your minimum requirements and explain that they are only the minimum. Require vendors to describe their redundancy scheme in detail and justify the type of links into and out of the ESInet. Consider using switch/router equipment from different manufacturers in your redundancy scheme at a given network layer. This reduces the likelihood that a software/firmware flaw or a security hole in one manufacturer's device will take down the entire network.
4. Require the ESInet to have much more bandwidth than you think you need now and at least a decade into the future. ESInets are required to support DiffServ (see *An Architecture for Differentiated Services*, RFC 2475 [8]). Routers must respect code points: functional elements must mark packets they create with appropriate mechanisms to ensure that high-priority traffic gets delivered, but having excess bandwidth is the simplest and probably the most effective way of ensuring that critical traffic always gets delivered. Require vendors to provide both – an ESInet that has a significant amount of excess bandwidth, implemented with network devices that support DiffServ and respect all DiffServ Code Points specified in NENA-STA-010 [4].
5. All shared facility networks (such as any IP network, or things like Metro Ethernet) are over-subscribed. This means that if the actual bandwidth available at a given

switch is 100 Mbit, and each customer connection is 10Mbit, the network operator will sell 12 or 15 or even more 10Mbit connections because it knows (correctly), that not all customers will need all of their bandwidth at the same time. The degree of oversubscription varies among suppliers. It matters how much oversubscription there is, of course. Dark fiber, Wave Division Multiplexed optical, SONET, and some forms of MPLS have isolation between customers such that each customer really can use all the bandwidth that the contract provides simultaneously. Obviously, this is better, but see point 3 above. Knowing how much oversubscription is provisioned is often hard to discern, but be aware that if the bandwidth is not isolated, everyone oversubscribes.

6. When planning networks for last mile to PSAPs, the above suggests that one should look extensively to find diverse facilities for the last mile. Use every possible physical path into the facility. If there is a cable system, connect to it. If it is within range of cellular networks, employ modems. If there is a copper wire facility that is separate from an optical cable, use both. Diversity and more bandwidth will substantially improve the availability of the PSAP. Networks that have two MPLS (or Metro Ethernet) connections from a single provider won't be anywhere near as reliable as one with eight connections to six providers using four different technologies.

3.7.1.7 Other Sections that Should be Reviewed

In addition to Section 3.7.1 ESInet (IP Transport Infrastructure), 9-1-1 Authorities developing an RFI/RFP for ESInet should also review the following sections of this document:

- Functional Elements and Services to Support Transition to NG9-1-1 (Section 3.9)
- SLAs and Other System Capacities and Performance (Section 3.10)
- Security and Cybersecurity (Section 3.11)
- References (Section 7)

3.7.2 Geographic Information Systems (GIS)

Prior to going out to bid for Geographic Information Systems (GIS) services, it is recommended that a 9-1-1 Authority assess any in-house GIS resources that may be able to provide any of the below provisions. RFPs seeking GIS services should incorporate the provisions contained in this section of the document that cannot be supported by in-house resources.

3.7.2.1 GIS Introduction

While the Geographic Information Systems (GIS) themselves may not be considered part of the RFP for an NG9-1-1 system, the geospatial information derived from them drives much of the NG9-1-1 system, including the ECRF and LVF. The NG9-1-1 Core Services are provisioned using a Spatial Interface (SI) described in NENA-STA-010 [4]. Thus, an

authority might issue a GIS RFP for 1) assistance in creation of NG9-1-1 GIS data and/or 2) procurement of the below listed items and/or 3) as part of the procurement of NGCS procurement. Most of the considerations in this section apply in either case.

Next Generation 9-1-1 (NG9-1-1) systems heavily depend on standardized, accurate, and up-to-date GIS data. Unfortunately, in many jurisdictions, existing GIS data falls short of basic accuracy standards and fails to meet the necessary business workflow requirements for maintaining precise and current information. Additionally, the required data footprint is directly related to the area covered by the Public Safety Answering Points (PSAPs) served by the procured system. As a result, aggregating data may be necessary either before or during the provisioning process, especially if the area involves contributions from multiple GIS data sources [17].

RFPs that include GIS deliverables should require a clear distinction between vendor and jurisdiction responsibilities. This could very well include the need for jurisdictions to maintain GIS data not only in a different format/schema, but also in a time-sensitive workflow environment. Therefore, it is important to fully understand the impacts that the implementation of NG9-1-1 will have on GIS stakeholders.

RFPs should specify what GIS systems are currently deployed in the service area contemplated by the RFP and require vendors to explain how they deploy the SI, which Quality Assurance/Quality Control (QA/QC) processes are supported, and how data is coalesced among the GIS systems that support NG9-1-1.

3.7.2.2 GIS Background Information

The implementation of an NG9-1-1 system within a PSAP's jurisdiction will have significant impacts on existing GIS and addressing business practices and workflows. Historically, local GIS data and addressing practices have evolved in silos between each local jurisdiction. The quality and structure of GIS data and workflows of local addressing have depended on the specific business drivers (Public Utilities, Public Works, Planning, Buildings and Permits, Assessor's Office, etc.) that leverage the data and are often unique to each jurisdiction. Further, the assumptions made in the i3 architecture about the availability of complete GIS systems and the ability to effectively update errors in that data in near real-time fashion are not reflective of all GIS enterprises at the local level.

GIS data developed for other jurisdictional requirements (e.g., land and tax records, Computer-Aided Dispatch [CAD], transportation) can provide a useful starting point for NG-9-1-1 but will rarely meet all the requirements. They will have different fields, store the data values in different forms and sometimes likely do not have all the necessary records.

In addition, while the PSAP community has been planning and preparing for NG9-1-1 for years, the same may not be true of the GIS community. Many GIS practitioners are just beginning to become educated about NG9-1-1 and the associated impacts. Depending on

the jurisdiction and associated organizational structure, the impacts to GIS and addressing entities will range from moderate to severe.

The implementation of an NG9-1-1 system will require new roles and responsibilities for personnel that may work outside of the PSAP organizational structure. In many cases, GIS and addressing functions will become part of the critical path workflow for emergency response. This will add new tasks, in addition to existing responsibilities. There may also be resource needs to support the data clean-up/creation phase and new workflows identified to maintain the data at the high precision and quality level required for NG9-1-1 systems. Therefore, involving and educating GIS and addressing stakeholders as early as possible is critical to successful implementation.

3.7.2.3 Regional Coordination

Migration to an NG9-1-1 environment may require regional cooperation and coordination. This will be required through the design, development, and deployment of the ESInet and NG9-1-1 Core Services, as well as the GIS datasets. While most GIS data responsibilities (quality control/maintenance) will fall inside a specific jurisdiction, there are certain tasks that require cross-border review.

Jurisdictional border and boundary questions that have not been resolved prior to NG9-1-1 implementation should be identified as high priority tasks. It will be necessary for the GIS authority and/or addressing authority to meet and resolve the PSAP and the Provisioning Boundary polygon issues.

Discussions related to organizational responsibilities and technical workflow processes can be difficult enough within a single jurisdiction. The challenges are compounded when multiple jurisdictions participate in the process. For these reasons, it is recommended that the identification of stakeholders and the coordination process start as soon as possible. Understanding the state of neighboring jurisdictions GIS data and how well it meets the needs of NG9-1-1 will have a direct impact on your timelines.

3.7.2.4 Creation or Upgrade of NENA-Required GIS Data Layers for NG9-1-1

As most deployed GIS data models do not meet the requirements of NG9-1-1 as defined in the *NENA Standard for NG9-1-1 GIS Data Model,* NENA-STA-006 [18], they will need to be upgraded to support NG9-1-1. NENA-STA-010, Appendix B [4] defines the ECRF/LVF provisioning data model. The ECRF/LVF requires two types of GIS data: service area boundaries and civic location data.

It is important to note which FCC designated phase is being procured per Code of Federal Regulations[3] when procuring NGCS as it will have a substantial impact on the order in

[3] CRF reference forthcoming once Report and Order, PS Docket Nos. 21-479 and 18-64, which were approved 7/19/2024 are filed in the national registry.

which GIS data requirements should be addressed. For phase 1, creation or updates to the required boundary files should occur first to support other NG9-1-1 needs (like Location Based Routing), before validating the currency and spatial accuracy of the centerline and address point layers. Further, if a transitional location database is deployed, this may drive assessing the priority of the centerline and address point layers. Ultimately, due to the time it will take to reconcile the legacy location values with the GIS location data elements, it would be advised to begin that process early.

However, if your jurisdiction is missing a RoadCenterLine layer and/or a SiteStructureAddressPoint layer, or these layers are incomplete, timelines need to be established, as they are very time consuming to develop and are critical to the incident location validation function. Consideration also needs to be given to how they will be maintained once developed. Boundaries (service and provisioning) are easier to develop and generally require less maintenance; however, determining their precise location (without gaps and overlaps) can be a lengthy process. For details, see *NENA Information Document for Development of Site/Structure Address Point GIS Data for 9-1-1*, NENA-INF-014 [19], and *NENA Information Document for GIS Data Stewardship for Next Generation 9-1-1 (NG9-1-1)*, NENA-INF-028 [17].

The ECRF/LVF does not require a wide variety of other GIS data layers which are useful for tactical dispatch or situational awareness. These may include layers such as aerial or satellite imagery, hydrography, topographic maps, fire hydrant locations, infrastructure maps, interior floor plans with elevation. The ECRF/LVF should be thought of as using a subset of available GIS layers, and not all GIS layers are used for other PSAP/ECC functions. The civic location dataset must fit the format of *NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF-US) Standard*, NENA-STA-004 [20], or NENA Next Generation 9-1-1 (NG9-1-1) Canadian Civic Location Data Exchange Format (CLDXF-CA) Standard, NENA-STA-029, CLDXF-CA. The planning for that is vital to the success of any NG9-1-1 deployment, but is beyond the scope of this document.

However, the RFP must inform proposers of the GIS data migration plan so that it may be integrated into the RFP response. The RFP response must detail any requirements the proposal assumes of the GIS systems beyond those contemplated in the GIS data migration plan. Proposals should also detail timelines from when a change is made in the GIS data to when NGCS will use the updated data. The RFP may wish to specify a maximum for that, such as daily, weekly, monthly, depending on the nature of the GIS maintenance within the jurisdiction.

Even though NENA-STA-006 [18] was designed specifically to detail the minimum requirements needed to support core ESInet functions, it is likely to be more detailed and complex than a locality's current database schema, while at the same time, additional data may be used locally that is not mandatory for NG9-1-1. This complexity will impact not only

the creation of the dataset, but also ongoing maintenance requirements. In part, this is due to the organic and non-standard driven nature of most GIS databases. The databases generally only contain data necessary to support the business needs of the departments they serve. To maintain continuity of operations with those existing applications, significant measures will need to be put into place to ensure that changes made to the databases and/or connections do not break other applications.

Lastly, in that there are likely GIS data requirements tied to individual NGCS functional elements that are not documented in a standard or information document, it is advised that 9-1-1 Authorities request these details as part of a bid and proposal process. Requiring that the GIS and location data at rest be standards based should be a consideration as a requirement, thus reducing any manipulation of the data being required when leveraged by the NGCS.

3.7.2.5 Quality Assurance/Quality Control (QA/QC)

RFPs should require vendors to explain what QA/QC processes are performed by any NGCS component, where and when the processes are performed, workflows for resolving the QA/QC results, and thresholds for acceptance by the functional elements. These need to be factored into the ongoing maintenance of the data by all stakeholders.

If the procurement is for GIS solutions to aid in QA/QC of the data, it is advised that there are checks addressing the need to compare the legacy location databases to the GIS data; this will be required to support the FCC phase 2 requirements.

It is advised that these requested details include any data model variances (additional elements and/or changes to the conditionality of an element in a published standard), geometric topology requirements with other spatial layers that are provided, and any standardization of attribute domains. Specific requirements may result in additional work that needs to be done by GIS data contributors and should be factored into an implementation timeline.

3.7.2.6 Spatial Interface (SI)

The SI is a standardized interface between the GIS data and the functional elements that consume GIS data, such as the ECRF, LVF, Mapping Data Service. The SI can be an integrated element in a GIS system or a standalone element with proprietary interfaces to GIS systems and standardized interfaces to the consumers of the data.

It may be helpful for a 9-1-1 Authority to provide guidance in an RFP as to any specifications they would require of a spatial interface that is being procured. Even though they can be standalone, it may be that an NGCS provider includes the SI as a required functional element in their offering. This is specifically important if the 9-1-1 Authority has an existing NG9-1-1 GIS data validation and/or aggregation project using a specific data model.

When procuring this functional element, it is essential to inquire about the specific NENA standards version to which the Spatial Interface (SI) is built. Additionally, consider asking whether the provider tracks potential changes to the standards and includes them in their product roadmap. This information can help you effectively assess viable solution offerings.

3.7.2.7 Mapping Data Service (MDS)

This is well specified in version 3 of NENA-STA-010 [4]. Consideration of how well the MDS performs as an INTERNAL map source is a key evaluation consideration. Performance issues dominate evaluation considerations as long as it meets the requirements of NENA-STA-010 [4].

3.7.2.8 MSAG Conversion Service (MCS)

The MCS is a simple subsystem and is probably best combined with other functional elements. As the MCS is provisioned by the SI, there really isn't much to consider other than performance. MCS is queried at call time by systems that need backwards compatibility, so transaction rates in this scenario are quite modest for modern systems. An MCS may also be used by OSPs for conversion of their existing legacy location records, as such, transaction rates for this scenario will likely be much more substantial. The MCS is required until every system in the PSAP that uses MSAG-style addresses is updated.

3.7.2.9 Location Validation Function (LVF)

The Functional Element Interface and Functional Information section of this document discusses the deployment options that can be selected as part of an NGCS procurement. As noted, the ECRF and LVF can be separate functional elements that must be provisioned with data by the spatial interface. It is important to ensure that data updates to both systems are synchronized with the same vintage of GIS data. How this is functionally accomplished by the SI may be a question to ask of proposers in an NGCS solicitation.

As a GIS consideration, it may be helpful to ask a bidder to provide a list of GIS data elements required for their LVF to function; if these differentiate from what is listed in the *NENA Standard for NG9-1-1 GIS Data Model* [18] or the inclusion designations are different from that document, this may have a cost implication to your GIS data contributors.

The LVF plays the role of ensuring that the source data in a LIS can be conveyed as a valid PIDF-LO object; inherently, this also requires both data sources to be compliant with the *NENA CLDXF-US Standard* [20]. It will be necessary to ensure 100% conformance to this standard for the source GIS data provided to the LVF for it to function properly.

3.7.2.10 Forest Guide Considerations

The Forest Guide is queried when the ECRF fails to find a location within its NG9-1-1 system and needs to discover call routing information outside of its domain, such as a

PSAP connected to a different ESInet outside of the area served by the ECRF (e.g., in a neighboring state or province).

For the purposes of procuring NGCS functional elements, it is recommended that you ask bidders to detail how they will accommodate 9-1-1 call routing transfers between your procured ESInet and another. For those that specifically detail the use of a forest guide function or the Forest Guide, it may be desired to know the source GIS data that will be needed or used to accommodate these lookups.

3.7.2.11 Other Sections that Should be Reviewed

In addition to Section 3.7.2 Geographic Information Systems (GIS), 9-1-1 Authorities developing an RFI/RFP for GIS should also review the following sections of this document

- Human Machine Interface (HMI) (Section 3.8)
- Functional Elements and Services to Support Transition to NG9-1-1 (Section 3.9)
- SLAs and Other System Capacities and Performance (Section 3.10)
- Security and Cybersecurity (Section 3.11)
- References (Section 7)

3.7.3 NG9-1-1 Core Services (NGCS)

RFPs seeking NG9-1-1 Core Services should incorporate the provisions contained in this section of this document.

3.7.3.1 Introduction

NG9-1-1 Core Services provide the intelligence to accept calls from Originating Service Providers (OSPs) and appropriately route a presented call to the appropriate destination. The first NGCS Functional Element to accept calls is the Border Control Function. The last NGCS FE to deliver a call is also the Border Control Function. A full description of the demarcation points for the ingress to and egress from NGCS can be found in *NENA Demarcation Points in NG9-1-1 Information Document*, NENA INF-003 [21]. In an end-to-end NG9-1-1 system, the appropriate destination can be NG9-1-1 functional elements for call taking, another NG9-1-1 system supporting a different jurisdiction, or an Interactive Media Response (IMR) device. Call signaling throughout NG9-1-1 uses the Session Initiation Protocol (SIP). In a transitional NG9-1-1 system, legacy gateways can be employed. A description of these legacy gateways can be found in Section 3.7.3.4.1 Functional Element Interface and Functional Information.

A few interfaces to NG9-1-1 Core Services are required to be provisioned on behalf of a 9-1-1 Authority. Examples of these are the ECRF, LVF, LIS (if hosted by the 9-1-1 Authority), and Policy Store. Time should be allocated to understanding these interfaces and clearly articulating requirements in an RFP. Note that the Human Machine Interface required to provision the Functional Elements is not defined in the NENA standards.

A more complete discussion of HMIs can be found in Section 3.8 Human Machine Interface (HMI).

The staff writing requirements for an NG9-1-1 Core Services RFP will benefit by being composed of persons knowledgeable in legacy and Next Generation networking, combined with knowledge of the NG9-1-1 and database requirements. Operations staff also need to be involved in establishing requirements for provisioning interfaces and must have an understanding of the background, skills, knowledge, and authority levels of personnel who will be assigned to use the provisioning interfaces.

3.7.3.2 Interdependencies with Other NG9-1-1 Components

The standards developed by NENA and other SDOs allow for a great deal of flexibility in how and when the 6 major components (NGCS, ESInet, Agency Systems, GIS Data, Call Handling, and MIS) of an NG9-1-1 system are procured. See Figure 3-1 Logical Overview of an NG9-1-1 System and other subsections of Section 3.7 NG9-1-1 System Elements for Procurement for details about those components.

While adherence to standards allows for decoupling of the procurement of components, system security and cybersecurity should not be addressed piecemeal. Security and cybersecurity should be viewed wholistically. A key element of system security is Public Key Infrastructure (PKI). To facilitate the adoption of PKI in NG9-1-1, the NG9-1-1 Interoperability Oversight Commission, in collaboration with NENA, has contracted with vendors to provide the required infrastructure. More about the PKI options available to 9-1-1 Authorities can be found on the NIOC's website (https://ng911ioc.org/library/). This topic and other information related to security and cybersecurity are also covered in Section 3.11 Security and Cybersecurity. Readers of this document should check the availability of other NENA documents covering this topic.

3.7.3.2.1 Interdependencies Related to Geospatial Information Systems (GIS) Data

As illustrated in Figure 3-1 Logical Overview of an NG9-1-1 System, the ECRF that hosts GIS data used in call routing and the LVF which hosts GIS data for use in validating addresses, are included in NGCS so if NGCS is being procured, these FEs are included. However, the interdependence between the GIS data and NGCS is an important consideration.

NENA's recommendation in preparation for a migration to NG9-1-1 includes developing a GIS database that meets or exceeds the NENA standards for quality and accuracy. Geospatial routing in an NG9-1-1 system depends on GIS data for the ECRF and LVF as well as systems and procedures for maintaining the quality of the data. If GIS data that meets the NENA standards is not available, on a transitional basis, call routing can be addressed based on current tabular data populated in a Location Database (LDB)

3.7.3.2.2 Interdependencies Related to the ESInet

The ESInet can be thought of as three segments: 1) the delivery of calls from the OSPs to the NGCS, 2) interactions between components within the NGCS, and 3) the delivery of calls from the NGCS to the NG-PSAPs.

ESInet segment 1 can be procured and implemented without any other NG9-1-1 components. A vendor can be selected to work with the OSPs to deliver their call while delivering them to the existing Legacy Selective Routers (LSRs). In most cases, this effort takes more time to execute than any of the other segments. GIS data and NGCS are not required to implement this segment.

ESInet segment 2 should be procured simultaneously with NGCS.

ESInet segment 3 can be procured after NGCS and segment 2 of the ESInet. It makes the most sense to deploy segment 3 when all PSAPs served by the NG9-1-1 system are SIP capable and ideally fully compliant with the NENA standards. Legacy PSAP gateways can be used to support the deployment of segment 3 of the ESInet to legacy PSAP call handling; however, this may be costly and require a transition later in the migration.

3.7.3.2.3 Interdependencies Related to Agency Systems

9-1-1 Authorities implementing NGCS should carefully consider the readiness of current Agency Systems to fully participate in NG9-1-1 systems. If current systems do not conform to the NENA standards, it is recommended that a plan be developed for upgrading these systems so they can fully participate in the NG9-1-1 system deployment. One option for upgrading the Agency Systems is to include the upgrade as part of the procurement. Another option is to migrate all Agency Systems prior to implementing NGCS. A third option is to implement the NG9-1-1 system and use Legacy PSAP Gateways to support the migration of PSAPs using Agency Systems that are not NG9-1-1-capable. This last option is costly, time-consuming, requires multiple migrations for the PSAPs, and is not recommended.

3.7.3.2.4 Interdependencies Related to MIS systems

Most NG9-1-1 capable MIS systems collect information from a variety of sources. Data collected from NGCS is primarily from the logging service. If NGCS is implemented prior to implementing a new MIS system, and if the MIS system is fully NG9-1-1 capable, logging information will be available.

3.7.3.2.5 Interdependencies Related to Emergency Incident Data Object (EIDO)

Because a call transferred from one PSAP to another includes a reference (a URI) to an EIDO that has caller location information and Additional Data that is available, all NGCS

elements that handle calls must ensure that EIDO references are passed intact to downstream elements. See NENA-STA-010 [4] for details on call transfers.

NENA Standard for Emergency Incident Data Object (EIDO), NENA-STA-021 [22], specifies the JSON object that is used to communicate important call and Incident related data. NG9-1-1 elements that handle incident data MUST support the EIDO standard.

3.7.3.3 Information to Provide Proposers about NGCS

NG9-1-1 standards are applicable to every jurisdiction. What drives the configuration in a jurisdiction is its specific requirements. It is recommended that the information below be provided to proposers in an RFP for NG9-1-1 Core Services.

1. Capacities related to the inbound side of the NG9-1-1 system need to be identified.
    a. Indicate the number of 9-1-1 voice calls needed to be handled annually. This includes calls originated on landline, wireless, VoIP, and all other networks that are mandated to provide 9-1-1 service.
    b. Specify the anticipated voice, text, and video call volume growth in the subsequent 5 to 10 years. This should include growth from an increase in the population or an increase in visitors.
    c. Peak call loads need to be addressed, and identify when the typical peaks occur.
    d. Identify the NG9-1-1 call types that the system is expected to handle natively, including audio, text-to- 9-1-1, photos, full-motion video, chat and real-time text sessions, and data from sensors and other automated devices. The projected volume of the various call types should be specified, as well as the growth in volume that is expected. All NG9-1-1 RFPs should require support for all media types listed in NENA-STA-010 [4].
2. Capacities related to the delivery of calls to the PSAPs need to be identified.
    a. Indicate the number of PSAPs or shared, hosted systems that will be supported by the Core Services.
    b. Identify the expected call volumes for each PSAP and the peak loads that need to be accommodated by media type.
    c. Initially, the number of PSAPs supported by the Core Services that are fully NG9-1-1-capable, the number that are IP-capable, and the number that are legacy need to be identified. Describe the plan and target schedule of the migration of all PSAPs to NG capability.
    d. Indicate the number of call takers that are normally assigned per shift at each PSAP.

e. List any other factors related to PSAPs that should be considered when establishing total system capacity.

3. Network bridging capacities and capabilities related to the transfer of calls to neighboring PSAPs using other legacy or NG9-1-1 systems need to be identified.
    a. Indicate the number of other NG9-1-1 and E9-1-1 systems the Core Services must be capable of transferring calls to and from. Call volume for each, as well as anticipated growth, should be specified.
4. State specific security requirements and require conformance to all relevant security mechanisms as described in NENA-STA-010 [4] including Single Sign-On, Data Rights Management, and TLS. State any requirements you have for what proposers must manage with respect to obtaining, assigning, and managing credentials.
5. Identify which jurisdictions and NGCS vendors must be included for interoperability. This may include NGCS systems deployed in bordering PSAPs/ECCs, regions, states, or countries. Requestor may desire to consider a requirement that the selected NGCS provider explain how they establish a standardized interface with the NGCS providers serving these other jurisdictions. It may be useful to ask responders to describe other existing implementations they have in production to support call transfers.

    NENA-STA-010 [4] specifies a Forest Guide for use in determining where to transfer calls that are outside of your jurisdiction. During the period before the Forest Guide is available, NGCS vendors may need to implement network-to-network interfaces to facilitate the transfer of calls to other ESInets.

    It should be noted that any interface may require additional, ongoing costs.
6. Finally, the RFP should cover requirements and preferences for the geographic location of the NGCS data centers. Technically, NGCS data centers can be deployed within the geographic boundaries of the 9-1-1 Authority issuing the RFP, within the county or state, or in the cloud as discussed in Section 3.6 Host, Manage, and Cloud Explained. The following should be considered when discussing NGCS Data center locations within the RFP
    a. NGCS Data centers should be geo-diverse. What level of geo-diversity can be achieved if the 9-1-1 Authority constrains the location of the data centers?
    b. What is the impact to the implementation timeline for each deployment option being considered by the 9-1-1 Authority?
    c. What State PUC and state security rules are in place within the jurisdiction that may limit options available to the 9-1-1 Authority?
    d. What FCC rules are currently in place or will be specified?

e. What are the cost implications for each of the options the 9-1-1 Authority wants to consider?

f. What security protocols are in place that affect the location of the NGCS data centers? This applies to geodiversity but also security aspects within the data center.

g. What security protocols are in place that affect the location of the data used by the NGCS, including but not limited to geospatial data for the LVF and ECRF, Policy Routing Rules for the ESRP, and 9-1-1 location data for LDB and LIS.

3.7.3.4 Information to Request from Proposers about NGCS

3.7.3.4.1 Functional Element Interface and Functional Information

NG9-1-1 Interfaces

The NENA Standards for NG9-1-1 define the interfaces between FEs. The NENA standards do not mandate specific deployment options for FEs. RFPs should require proposers to describe how each of the FEs they provide conforms to the NENA standards and how the FEs are deployed. A network or solution diagram that clearly maps out the end state for the NG9-1-1 Core Services should be mandatory for all RFP responses. Except where noted, all functions below should be visible on the solution diagram.

NGCS

These are some considerations for what FEs in the call path may be valuable to include in an RFP and how to evaluate the responses:

1. BCF

    a. BCFs typically have commercial Session Border Controllers in them. Commercial SBCs are designed by a typical carrier's maxim of "default deny": when in doubt, meaning don't allow a call in. 9-1-1 doesn't work that way; it is "default allow." Only under extreme conditions should the BCF deny a call. On the other hand, the BCF is the primary line of defense on attacks against the ESInet and NGCS. Understanding how a proposed BCF balances these issues is essential to properly compare proposals. Take care to require the BCF functions for "Bad Actor" defined in NENA-STA-010 [4], as these require capabilities beyond those that commercial SBCs provide.

    b. DDoS (Distributed Denial of Service Attack) and TDoS (Telephony Denial of Service) mitigation is a significant issue for any proposal. Each proposal must specify how the proposed solution would survive the largest feasible attack. In general, it is not feasible to have the BCF perform this function itself. It typically requires a DDoS/TDoS mitigation service in addition to significant

capability at the BCF itself to recognize and filter attack traffic from legitimate traffic. The manner in which attack traffic is handed off between the BCF and the mitigation service is a key part of a system design and should be reviewed as part of any proposal evaluation.

2. ESRP
    a. Take particular care to require/evaluate how well proposals conform to the Policy Routing Function portion of NENA-STA-010 [4]. Development of appropriate policies is challenging, and any tools or assistance that the vendor provides should be explained and understood. As with ECRF/LVF, the ESRPs may be deployed hierarchically (state/region/local), and the RFP should specify what is required. 9-1-1 Authorities need to understand how the proposal manages to maintain the desired availability of the SIP call chain, and specifically, if an ESRP is call stateful (and most are), how a failure of an ESRP can be recovered without affecting calls that are established and calls that are in the process of being set up. It is inevitable that a failure early in the call setup will cause the call setup attempt to fail (but should be retried at the origination side). Implementations vary as to how well they handle failures, and 9-1-1 Authorities need to understand how a particular implementation proposal maintains availability. Note that the very definition of availability is part of this discussion: if a call fails to set up because an instance of an ESRP fails, but other ESRP instances are available to take succeeding call attempts, is that an availability SLA miss? Is that failure accounted for in any SLA?
    b. Understand how callbacks are handled and what role the ESRP plays. Version 3 of NENA-STA-010 [4] extends mechanisms for how callbacks are handled and should be considered when evaluating responses.
3. Policy Store
    a. This is a key component of a successful NG9-1-1 deployment. It is desirable that there be a single Policy Store that contains all policies for any entity, and all FEs that need a policy would fetch it from the Policy Store. It is acceptable to combine a Policy Store with another FE. Any tools or processes that the vendor provides to help create policies might influence selection. As it is such a key element, its availability (through redundancy) is essential to understand.
4. ECRF
    a. Both an internal (to the ESInet) and an external ECRF may be required. These really need to be separate as they have different content. The external ones need significant protection against a DDoS attack. It is desirable to have

multiple instances of both the internal and external ECRFs. Internal (and possibly external) ECRFs can be hierarchical (local, regional, statewide). The RFP may wish to specify the hierarchy desired. Where there are only higher-level ECRFs, then coalescing of data is necessary, because the source data is distributed among many local GIS systems. Coalescing can be done at an SI function or can be done in the ECRF itself. The proposal must discuss how the proposer coalesces data. It should also discuss quality assurance issues and the time duration between a GIS update and the implementation of the new call routing. There is a trade-off between achieving adequate QA and implementing a timely update cycle. It is desirable to be ABLE to achieve online, real-time updates in which time from update to routing change is measured in seconds, however, this must be balanced against QA process requirements.

b. The capacity of the ECRF is generally not an issue, but it is affected by the DDoS problem. DDoS mitigation is not an exact science and does not activate immediately. Thus, the ECRF has to be able to withstand some level of attack traffic. Proposers should state how they mitigate attacks and how the ECRF copes with whatever the DDoS mitigation does not handle.

5. Forest Guide

   a. The Forrest guide is used to facilitate interoperability between ESInets for call transfers.

   b. The NENA Glossary [1] defines the Forest Guide:

      The Forest Guide is a special instance of a LoST server. It is part of the LoST (Location-to-Service Translation) Protocol (RFC 5222) query process and allows client functional elements to discover call routing information outside of its domain (typically their ESInet or state level ECRF/LVF).

   c. To perform its intended purpose, the expectation is that GIS data for NG9-1-1 Systems must be provisioned in the Forest Guide by the authoritative source of the GIS information.

More information about the required GIS data and the process for creating and maintaining it can be found in Section 3.7.2.4 Creation or Upgrade of NENA-Required GIS Data Layers for NG9-1-1.

6. LIS (if not hosted by OSP)

   a. By standard, LISs really need to be operated by the OSP. Legacy systems use LNGs, and LNGs have Location Servers, which are a form of LIS. The LNG is often part of an NG9-1-1 procurement, but a real LIS for a migrated Origination Network should be the responsibility of the OSP. A LIS for an

entity like a cable system or passive optical network operated by a telco should be provided by the network and not the 9-1-1 Authority. "Should be" and "is" may not be the same, and it may be that the 9-1-1 Authority is forced into providing a LIS. Evaluating LIS proposals mostly deal with capacity, strategies for periodic revalidation and provisioning interfaces, and processes (noting that because NENA-STA-010 [4] assumes the LIS is operated by the Origination Network, it doesn't specify a provisioning interface).

7. Additional Data Repository (if not hosted by the OSP)
    a. The Additional Data Repository (ADR) is a very simple database. The 9-1-1 Authority may need to provide an ADR for OSPs that will not do it themselves. Evaluation of capacity (how many records) and provisioning interfaces (since NENA-STA-010 [4] assumes the OSP or third parties will operate the ADR) must be taken into consideration.
8. Service/Agency Locator
    a. All ESInets need a Service/Agency Locator. This is a simple database with a trivial interface, but since it may be consulted during an emergency call, it has to be reliable. The provisioning of the Service/Agency is not specified, and may well be manual, so evaluating how records are maintained is significant.
9. Logging Service
    a. The logging service in NG9-1-1 is considerably different from classic loggers used in 9-1-1 systems for decades. There is a great deal of standardization, not only on the recording side, but also on the retrieval side. As new standards evolve, they often add new LogEvents, which are the standardized data models for what the logging service stores. The logging service is defined to be able to be in the ESInet, or in a PSAP, or both. Conformance to standards is essential. Because the logging service must record multimedia, the capacity of the system is much greater than that of older loggers. Furthermore, since many functional elements log events, the transaction rate the logging service has to achieve is significantly higher than in older systems and must be carefully considered in evaluating responses.
    b. Because the retrieval system is standardized in NENA-STA-010 [4], it should be possible to develop a wide variety of applications that can mine the data for events of interest and provide interesting ways to view/access the data. Making sure the proposed logging service meets all the standards in NENA-STA-010 is essential to being able to take advantage of such applications.

3.7.3.4.2 Operational Elements (Deployment Options)

1. LVF
    a. All the above statements on ECRF apply to the LVF. The ECRF and LVF can be combined. The argument for making them separate is that the ECRF is real-time call routing and the LVF is offline, before the call validation, and combining them complicates the difference between them. The argument for combining them is that they are exactly the same function, with the same interface and the same provisioning. Every route request could, theoretically, request validation, and every validation request returns a route. Either is satisfactory, but if they are separate, the proposer should describe the differences between them in terms of capacity, DDoS mitigation, and their effect on cost. If combined, the proposer must describe how the capacity to accomplish both tasks is accomplished.
    b. Periodic revalidation of LIS content will overwhelm the use of the LVF from initial LIS pre-load validation, so the capacity of the LVF is gated on the size and revalidation frequency of the LISs it serves. The proposal must describe how this is accounted for. There are new functions in development that will change how validation is kept current, significantly reducing the need/frequency to revalidate. Proposers should be asked when they will support these new capabilities. Note that the LIS will have to implement the new functions in order to take advantage of them.
    c. Consider how you will handle Additional Data about a Location, for which there is provisioning in the LVF for querying by location to determine if such data exists. Proposals should specify how such data will be provisioned. Note that the LVF itself uses the SI to provision all data, including the data associated with Additional Location Data, but the proposal should be evaluated to understand the entire process of storing and retrieving the data.

3.7.3.4.3 Migration Plan Options

Defining the NG9-1-1 system to replace the existing E9-1-1 system is critical. The topics above, if covered properly, should provide the necessary level of definition and set expectations with proposers during the procurement process. Equally important is defining how the migration to the NG9-1-1 system will be achieved. There are several migration strategies that have been used successfully by 9-1-1 Authorities. These include migrating OSP types as a group, usually beginning with wireless carriers. Migrating geographically—county by county or region by region—has also been employed. The 9-1-1 Authority should specify in the RFP any preferences they may have for the migration and any context that will be helpful to proposers. Proposers will then be in the best position to propose a

migration plan. 9-1-1 Authorities should make proposers aware of any additional expectations and note any limitations of which the vendors should be aware.

3.7.3.5 NG9-1-1 Core Services Reference Documents

Use Section 7 References to identify valuable documentation on NG9-1-1 Core Services.

In addition to Section 3.7.3 NG9-1-1 Core Services (NGCS), 9-1-1 Authorities developing an RFI/RFP for NG9-1-1 Core Services should also review the following sections of this document:

- Human Machine Interface (HMI) (Section 3.8)
- Functional Elements and Services to Support Transition to NG9-1-1 (Section 3.9)
- SLAs and Other System Capacities and Performance (Section 3.10)
- Security and Cybersecurity (Section 3.11)
- References (Section 7)

3.7.4 NG9-1-1 PSAP/ECC Functional Elements (FEs)

RFPs seeking NG9-1-1 PSAP/ECC FEs should incorporate the provisions in this section of the document.

3.7.4.1 Introduction

The NGCS defines a PSAP as a service composed of multiple FEs that interacts with its external interfaces, including:

- SIP call interface
- Media interfaces
- Call queues
- Multiple SUBSCRIBE/NOTIFY event packages (ElementState, ServiceState, AbandonedCall, DequeueRegistration, QueueState, PSAP ServiceState/Security Posture, etc.)
- Time
- Test Call
- Call Diversion
- Location to Service Translation (LoST)
- HTTP Enabled Location Data (HELD) and SIP location subscriptions
- Mapping Data Service interfaces
- Discrepancy Reporting

These external interfaces are defined or referenced in NENA-STA-010 [4]. Details on the PSAP/ECC's use of these external interfaces are defined in *NG9-1-1 PSAP and ECC Specifications for the NENA i3 Solution*, NENA-STA-023 [23].

The NENA-STA-010 [4] and NENA-STA-023 [25] specify Functional Elements, not systems. An FE is part of a system that performs some function and has one or more interfaces. For

example, the hot-water hose on a washing machine could be considered an FE—it delivers hot water to the machine via a standardized hose coupling interface. But the hot water hose doesn't wash clothes. It must be combined with other FEs like a cold-water hose, tub, agitator, drain hose, and other FEs into a system that washes clothes and has a user interface that lets you control its functions.

IMPORTANT: Agencies do not buy FEs—they buy systems that incorporate the FEs. The standards specify FEs that interface to other FEs so that vendors can combine them into useful systems that will interoperate with systems from other vendors.

If you buy a Call Handling System (CHS), it will implement all the call and media-related interfaces required for a Call Handling FE, but also the Incident interfaces of an Incident Handling FE. A CAD system will implement both Dispatch and Incident Handling FEs. Both need Incident Handling because both systems can change the status of the incident and must communicate this to each other, and to other systems. A vendor can implement all these interfaces and functions into a single system that does it all, or separate them into discrete systems that implement the standard interfaces.

The FEs that make up a PSAP are defined in NENA-STA-023 [23]. FEs are typically combined into systems that provide a user interface along with the specified functionality and interfaces. NENA-STA-010 [4] and NENA-STA-023 [23] don't specify user interface aspects, only the required functions and interfaces that allow the systems to interoperate with FEs implemented in other systems.

RFPs seeking any system that incorporates a PSAP/ECC FE should ensure that the implementation conforms to all of the applicable requirements in the General Specifications section of NENA-STA-023 [23].

IMPORTANT: A system that implements multiple FEs may use internal mechanisms to share data—but the system must implement the required standard interfaces so it can share data with external systems. A system that doesn't provide interfaces that the standard says must be supported should have its interoperability questioned. Lack of a required external interface could render the system unusable with systems from other vendors. Optional interfaces are just that—optional and not required. Optional interfaces can enable additional functionality and should be considered for any additional value they can provide.

3.7.4.2 Emergency Incident Data Object (EIDO)

EIDOs are used to exchange Incident data within the PSAP, with other PSAPS, and with other authorized agencies and entities. The EIDO also provides caller location and Additional Data information when a call is transferred. It is critically important that NENA-STA-021 [22] is supported by every element that must communicate Incident data, including, but not limited to, those that implement NG9-1-1 Call Handling, Dispatch, Incident Handling, and Responder Data Services functions.

The protocols used to exchange EIDOs between FEs, Agencies, and other entities are defined in *NENA Standard for the Conveyance of Emergency Incident Data Objects (EIDOs) between Next Generation (NG9-1-1) Systems and Applications,* NENA-STA-024 [18].

All systems that exchange Incident data in an NG9-1-1 PSAP/ECC must support the EIDO data object and the EIDO Conveyance interface, and RFPs should clearly state this.

3.7.4.3 Transition Issues for NG9-1-1 PSAP/ECC

Transitioning from E9-1-1 systems to NG9-1-1 systems presents challenges that both the vendor and user must consider. An NGCS must exist before an NG9-1-1 PSAP can take calls from it, but there are other issues that occur wholly within the PSAP or ECC when transitioning to NG9-1-1.

The issues occur when upgrading one system to NG9-1-1, and other systems that interface to it are still legacy systems and don't have the required standard interfaces. For example, a legacy CAD typically has an ALI interface for caller location, but an NG9-1-1 Call Handling system has an EIDO interface for location.

The *NENA Transition to i3 PSAP Standard*, NENA-STA-049 [25] specifies legacy interfaces that certain NG9-1-1 systems must implement to work in transitional implementations and provides useful advice for situations where the legacy interfaces required may vary from Agency to Agency. Those writing RFPs for NG9-1-1 Call Handling, Dispatch, and Logging Services should read NENA-STA-049 [25] prior to writing the RFP, and should require respondents to explicitly state whether, and how, their implementation conforms to NENA-STA-049 [25] and how the transition from legacy to NG9-1-1 will be accomplished.

It is also true that NENA standards continue to evolve over time, and a vendor's implementation may be evolving as well. 9-1-1 Authorities should demand that systems are as conformant to the evolving standards as possible with the expectation that they will be brought into conformance with new standards as they are released. Require vendors to discuss how they plan to evolve their systems as the standards evolve and how they will handle the required upgrades once they are approved. This is an appropriate topic for a Service Level Agreement (SLA) between the vendor and the 9-1-1 Authority.

3.7.4.4 Background Information

With the transition to NG9-1-1, an agency releasing an RFP should anticipate investing time in conducting background research related to NG9-1-1 and the network infrastructure that supports it. Background research should be conducted on the following:

- IP Security: In legacy PSAP environments, network connectivity is typically via a closed system with little or no access to any external networks (i.e., a single connection to one external network through a firewall). Often, system providers prohibit equipment they did not supply from being connected to the systems they did supply. In the transition to NG9-1-1, call handling, incident handling, dispatch,

and other systems, as well as other functional elements that interconnect with them, must be connected via a secure network. An NG9-1-1 PSAP network has the same stringent requirements as the ESInet to which the PSAP is connected.

- Governance: Transitioning to NG9-1-1 moves agencies towards interoperability. NG9-1-1 PSAP systems will be part of this ecosystem. Time should be taken to review and understand state, regional, and local laws and policies that may need modification to facilitate this type of system.
- As with other aspects of NG9-1-1, procurement of NG9-1-1 systems may require agencies to review existing procurement vehicles to ensure the language is current and supports acquisition of advanced NG9-1-1 systems.
- Due to the distributed nature of i3 networks, the architecture of the i3 PSAP Network may allow interconnections to networks with different security policies. For example, if connectivity to the FBI's Law Enforcement Online (LEO) [26] database and systems or to the National Crime Information Center (NCIC) [27] is required, then compliance with the FBI's Criminal Justice Information System (CJIS) security policy [28] will have to be supported. i3 PSAP Networks that communicate with local, state, and national networks will likely have to accommodate various and, possibly, conflicting, security policies.

3.7.4.5 NG9-1-1 PSAP/ECC Interdependency with Other NG9-1-1 Components

An NG9-1-1 PSAP/ECC depends on an NGCS to deliver calls and Incident data to it, therefore the NGCS must be implemented first. If a conformant NGCS has been implemented on a conformant ESInet, then NG9-1-1 PSAPs can be implemented. There are internal issues to be aware of when implementing an NG9-1-1 PSAP in stages—see Section 3.7.4.3 Transition Issues for NG9-1-1 PSAP/ECC for details.

NG9-1-1 PSAP systems and services require a conformant PSAP network that meets the same stringent requirements as the ESInet that hosts the NGCS. Support for Transport Layer Security (TLS) and Differentiated Services (DiffServ) is required on the PSAP network. The PSAP network will have lower bandwidth requirements than the external ESInet, but will definitely require more bandwidth than a legacy PSAP/ECC. The performance of NG9-1-1 PSAP systems and services is dependent upon the PSAP network, so the network requirements must be studied beforehand, and the network must be designed to carry NG9-1-1 traffic in the most demanding Incident that can be expected. Requirements for ESInets are found in NENA-STA-010 [4] and NENA-INF-016 [7].

PSAP and ECCs use identity certificates traceable to the PSAP Credentialing Agency (PCA) as described in Section 3.11.1 PSAP Credentialing Agency and Certificate Authorities. Other NG9-1-1 Components that must be Implemented prior to or in conjunction with Core Services. The Agency's responsibilities for management and renewal of its certificates are virtually identical to those for an Agency that manages an NGCS system. A PSAP or ECC

should contact the manager of the NGCS system for information on obtaining the necessary certificates.

An NGCS can serve a legacy PSAP through a Legacy PSAP Gateway (LPG). See the discussion about Legacy PSAP Gateways in Section 3.7.5.4.2 Functional Element Interface and Functional Information for more information.

NG9-1-1 Call Handling will generate detailed log messages called LogEvents that contain a plethora of call statistics and details that can be used to manage the PSAP better. Implementing an NG9-1-1 Logging Service concurrently with Call Handling allows management to take advantage of the LogEvents for analysis and troubleshooting during the transition. The LogEvent Replicator forwards LogEvents to other systems like an NG9-1-1 Management Information System (MIS). Consideration should be given to implementing the NG9-1-1 Logging Service and MIS concurrently with Call Handling.

3.7.4.6 Information to Provide Proposers about NG-PSAP

Responding to RFPs for NG9-1-1 PSAP/ECC systems requires a thorough understanding of the Agency's planned NG9-1-1 infrastructure, current and projected call and Incident volumes, staffing, transition plans, and any anticipated constraints on the project. 9-1-1 Authorities should strive to provide as much accurate information as possible to potential respondents because it will significantly increase the quality of the responses submitted. The 9-1-1 Authority should provide a fair amount of detail in the following major areas:

1. Proposed Network Architecture
    a. LAN/WAN design
    b. Resiliency scheme(s)
    c. Network transition plan(s)
    d. Any legacy infrastructure that impacts the RFP
2. PSAP/ECC Model
    a. Standalone PSAP, ECC, or combined agency
    b. Existence of secondary PSAP/ECC
    c. Hosted, Managed, or Cloud PSAP configurations[4]
    d. Interoperation, convergence, collocation, or cooperation with other Agencies
3. Operational Details
    a. Staffing (average, peak)
    b. Number of positions
    c. Call and/or Incident volume (average, peak)
4. Constraints
    a. Procurement method
    b. Budgetary/funding

[4] A Hosted configuration is one where multiple agencies access functions (e.g., Call Handling or Dispatch) provided by an external server or service.

c. Technical constraints, transitional issues (e.g., legacy equipment interfaces)
d. Calendar/timing
e. Any other constraints that would likely affect implementation.

3.7.4.7 Information to Request from Proposers about NG-PSAP

If proposing a Hosted configuration (including a "cloud" implementation) or any other configuration where FEs are shared by multiple Agencies, RFPs should explicitly require the following:

- Allow each Agency to have its own policies, including security policies.
- Allow each Agency to control access to configuration data specific to that Agency.
- Not allow the provisioning of an Agency to affect the provisioning of another Agency.

Because NG9-1-1 PSAP/ECC systems can incorporate multiple FEs, the proposer must state clearly which FEs are included in their system(s). FEs are allowed to communicate internally within a system, but must always implement the standard interfaces so they can interoperate with FEs from other vendors. Require proposers to state clearly that their system implements the standard interfaces of each FE incorporated in the system, and if any are not implemented, how the absence could affect interoperability with systems from other vendors.

The following sections describe NG9-1-1 PSAP/ECC FEs defined in NENA-STA-023 [23] along with important details that RFPs should request. Some NG9-1-1 FEs did not exist in E9-1-1 and may not be readily available at the time of an RFP for major systems like Call Handling, CAD, or Logging Services. FEs that are unavailable can be procured later in the process and should be required to interoperate with FEs acquired earlier. To achieve interoperability, it is critical that all FEs and Services conform to all the required interfaces specified or referenced NENA-STA-023 [23]. The Document Terminology section of NENA-STA-023 [23] describes how required functions and interfaces are identified in the standard.

The PSAP/ECC Logging Service relies on LogEvents from other PSAP/ECC FEs and Services, so it is important to require all respondents to attest that any offered FE/Service implementation will log all required LogEvents.

3.7.4.7.1 Call Handling Systems

The Call Handling Functional Element (CHFE) is the key FE in a Call Handling System and is responsible for processing calls. This includes the SIP interface to the NGCS network over which emergency calls are received and MAY interface to the Agency's other communication systems and networks (an administrative PBX, Public Switched Telephone Network [PSTN], etc.) via an External Switching System (ESS) SIP interface. The CHFE must support all media types required for PSAPs by NENA-STA-010 [4].

To process the underlying Incident and related data being reported by a caller (e.g., the ability to display and update Incident data such as location) an Agency must have an Incident Handling FE (IHFE) in addition to the CHFE. The CHFE and IHFE each have distinct responsibilities in support of call and incident handling. Dispatch (described below) also requires the IHFE. The IHFE may be incorporated in the Call Handling system and/or Dispatch system, implemented separately, or even shared by the two systems, but the IHFE is a critical part of a Call Handling or Dispatch system. The IHFE is described separately below.

NENA- STA-023 [23] specifies how the CHFE interoperates with the NGCS and with other FEs in the PSAP/ECC in great detail. RFPs should require proposers to state clearly that their implementation supports all the interfaces and functions defined in NENA-STA-023 [23] that are not marked as optional. A good practice is to require a response for each interface or function that states whether the implementation supports the required function or interface, and if not, when it will be supported. If the vendor does not intend to support a required function or interface, the vendor should be required to state so and detail any impacts that the decision may have on the 9-1-1 Authority's project.

3.7.4.7.2 Computer-Aided Dispatch (CAD)

Computer-Aided Dispatch (CAD) systems are used to assign and dispatch resources for an Incident and to update Incident state information during the response to an active Incident. A CAD system is an example of a system that incorporates multiple FEs. This document defines a Dispatch FE and an Incident Handling FE (IHFE) that standardize communication between these FEs and other FEs that deal with the Incident state. The CAD's Dispatch FE defined in this document manages resources (emergency responders, equipment, etc.) and is responsible for notifications and logging of Incident state changes relative to those resources. The CAD's IHFE is responsible for receiving notifications and logging all other Incident state changes handled by the CAD system. Of course, assigning resources changes the Incident state. A CAD system that conforms to this specification is expected to implement both a Dispatch FE and an IHFE. Per the Dispatch FE and IHFE specifications below, the EIDO is the format used to communicate Incident state with external FEs, noting that an IHFE and Dispatch FE bundled in a CAD system might communicate Incident state internally by some other means. The key is that a CAD system must support the EIDO and EIDO Conveyance for communication with other systems.

NENA- STA-023 [23] specifies EIDO requirements that apply to all systems that share Incident data, in an Emergency Incident Data Object (EIDO) section. RFPs should require Call Handling, CAD, and other systems that share Incident data to fully conform to the requirements in the EIDO section.

3.7.4.7.3 Dispatch Functional Element

The following are the primary functions of the Dispatch Functional Element (Dispatch FE):

- Recommend appropriate resources (emergency responders, equipment, etc.) available for an Incident.
- Assign emergency responders and other resources to an Incident.
- Manage the inventory and status of resources.
- Provide and receive relevant resource information for the agency and responders.
- Monitor and log all transactions associated with resources.

The Dispatch FE is the key component of a CAD system and functions with the IHFE (below) to interoperate with other systems that use Incident data.

3.7.4.7.4 The PSAP/ECC Incident Handling FE (IHFE)

A PSAP IHFE's responsibility starts when an incident is created, typically when a call is received, or an incident is reported via other means. When a call is an NG9-1-1 call, it will be accompanied by a unique Incident Tracking Identifier which is used to track the Incident throughout its lifecycle.

The IHFE is responsible for handling Incident state changes for systems like Call Handling and CAD, and for notifying other FEs and Services of the changes via the EIDO Conveyance mechanisms defined in NENA-STA-024 [18]. RFPs seeking Call Handling or CAD systems must require respondents to state how the proposed system satisfies the IHFE functions and interfaces specified in NENA-STA-024 [24].

3.7.4.7.5 Presence Server FE

The Presence Server is a Functional Element (FE) responsible for receiving Agent activity state information from other FEs, storing it, and distributing agent presence information to subscribing entities. The Presence Server FE accepts AgencyID, AgentID, ActivityState (including ReasonCode information) from other FEs responsible for determining the state of agents.

The Presence Server FE may be implemented in a standalone system or bundled with other FEs in a more complex system. It provides critical information required to effectively manage PSAP/ECC Agents and to drive analytics applications. The Presence Server FE supports richer detail about Agent activity than has traditionally been available to PSAP/ECC managers. RFPs seeking Call Handling systems should consider seeking Presence Server functionality as well.

3.7.4.7.6 Media Proxy FE

One-way, non-interactive media comes from two sources:

- Responders via the responder data channel (e.g., body and dash cameras)
- Public or private sources via Additional Data (e.g., surveillance cameras, smartphone video recording)

The Media Proxy FE acts as a proxy between the media source and the Agent or Responder accessing the media and ensures that the media is recorded in the PSAP/ECC. RFPs seeking a Media Proxy should require respondents to attest that their implementation conforms to the specifications in the Media Proxy Functional Element section of NENA-STA-023 [23].

3.7.4.7.7 Management Console FE (MCFE)

The MCFE supports important management functions for the PSAP and utilizes important event mechanisms specified in NENA-STA-010 [4]. As with all FEs, the MCFE could be implemented in a standalone application or bundled with other FEs into a complex system. PSAPs/ECCs seeking Management Console functionality should require respondents to attest that their implementation conforms to the Management Console section of NENA-STA-023 [23]. Major functions of the MCFE include the following:

Per NENA-STA-010 [4], the NGCS treats the PSAP as a "Service" that has a PSAP Service State from the IANA Service State registry that includes Normal, Unstaffed, Overloaded, etc. The MCFE manages and reports PSAP Service State to subscribers such as ESRPs.

- The MCFE can manually influence the state of a specific queue. Examples include changing a diversion queue from Standby to Active, or temporarily disabling a queue for some reason.
- NENA-STA-010 [4] defines the Discrepancy Reporting mechanism for standardized reporting of issues encountered by FEs. The MCFE receives all Discrepancy Reports from outside entities and forwards any Discrepancy Reports from PSAP FEs that target any outside entity.
- The MCFE MAY implement a Policy Editor as defined in the Policy section of NENA-STA-010 [4] for managing PSAP/ECC policies.
- The MCE FE implements important monitoring functions that include the following:
    - Monitors the LogEvent web service interface, to receive copies of Monitors the LogEvents from the LogEvent Replicator.
    - Monitors the Subscribe to ServiceState/SecurityPosture of all Services in the PSAP.
    - Monitors the Subscribe to ElementState for every FE in the PSAP
    - Is capable of subscribing to ServiceState/SecurityPosture of a provisioned list of Services outside the PSAP.
    - Subscribes to provisioned ESRPs' ESRPNotify event so it knows if calls are being diverted.
    - Subscribes to Agent Activity State notifications provided by the Presence Server.
    - Subscribes to the QueueState of every queue managed by the PSAP's CHFE (required by STA-010).

3.7.4.7.8 Responder Data Services (RDS) FE

The Responder Data Services Functional Element (Responder Data Services FE) is an optional FE that can be used to transfer data (including streaming media) between a PSAP and emergency responder devices. Responders may be an individual agent, identified with an Agent ID, or may be a unit, identified with a Unit ID-Common, as defined in NENA-STA-021 [22]. The advantage of the RDS FE is that it standardizes data communications between the PSAP/ECC and Responder devices and applications.

RFPs seeking RDS FE functionality should require vendors to attest that their implementation conforms to the specifications in the Responder Data Services Functional Element section of NENA-STA-023 [23].

3.7.4.7.9 The PSAP/ECC Logging Service

The Logging Service defined in NENA-STA-010 [4] provides critical logging and recording services to the PSAP. Every i3 PSAP MUST have a Logging Service. A PSAP MAY have its own Logging Service, or it MAY use a Logging Service provided in the NGCS. A Logging Service shared by multiple Agencies should adhere to the requirements for Hosted and "cloud" systems in Section 3.6 Host, Manage, and Cloud Explained in this document.

The Logging Service may store Criminal Justice Information, and is expected to conform to the FBI's Criminal Justice Information System (CJIS) security policy [28].

The PSAP/ECC Logging Service receives LogEvents from PSAP/ECC FEs and Services and creates a detailed record of call and Incident processing in the Agency. RFPs that seek any PSAP/ECC FE or Service should require all respondents to attest that any such FE/Service implementation will log all required LogEvents.

RFPs seeking a PSAP/ECC Logging Service should also seek a LogEvent Replicator in order to support the management and monitoring functions of the MCFE and MIS (see below).

3.7.4.7.10 The LogEvent Replicator FE

The LogEvent Replicator is defined in NENA-STA-010 [4]. It sends copies of LogEvents it receives from the Logging Service to applications that use the events for various purposes, like displaying the status of calls, agents, and services, or for monitoring and analysis purposes, thereby relieving the Logging Service of the additional burden of replicating to such applications. The LogEvent Replicator is required in order to send copies of LogEvents to the MCFE to support its management and monitoring functions.

3.7.4.7.11 Management Information System (MIS)

The LogEvent Replicator described above provides copies of LogEvents for MIS reporting and analysis, so RFPs seeking MIS should include a LogEvent Replicator if not already present. The Management Information System (MIS) Functional Element provides reporting

services based on data collected from FEs. The types of collected data may include the following:

- Communications processing data generated by FEs
- Authentication events generated by FEs
- Call and Incident state change information
- Data access events

RFPs seeking MIS should require vendors to attest that their implementation conforms to the requirements in the Management Information System section of NENA-STA-023 [23].

3.7.4.8 SLAs and Other System Capacities and Performance

At a minimum, metrics used for statistical measurements should conform to the *NENA NG9-1-1 Call Processing Metrics Standard*, NENA-STA-019 [29].

3.7.4.9 Other Sections that Should be Reviewed

In addition to Section 3.7.4 NG9-1-1 PSAP/ECC Functional Elements (FEs), 9-1-1 Authorities developing an RFI/RFP for NG9-1-1 PSAP/ECC Functional Elements should also review the following sections of this document:

- Human Machine Interface (HMI) (Section 3.8)
- Functional Elements and Services to Support Transition to NG9-1-1 (Section 3.9)
- SLAs and Other System Capacities and Performance (Section 3.10)
- Security and Cybersecurity (Section 3.11)
- References (Section 7)

3.7.5 Management Information Systems

As Management Information Systems (MIS) are evolving, 9-1-1 Authorities should be seeking MIS services to incorporate the provisions contained in this section.

3.7.5.1 Introduction

An MIS provides critical analytical insights needed to properly manage and evaluate the effectiveness of the 9-1-1 network (legacy or ESInet) and call handling equipment (CPE or CHFE) solutions employed to process all calls entering or exiting the 9-1-1 system, including administrative calls, language translation services, etc.

There are two aspects to MIS in an NG9-1-1 world: PSAP-specific analytics related to call handling service delivery performance to the public and NGCS-specific analytics related to call processing and routing. This section addresses both ESInet-specific MIS and PSAP-specific analytics, which apply to both NG9-1-1 and legacy systems. The guidance provided in this section may equally apply to stand alone or shared systems.

3.7.5.2 NG9-1-1 Components Needed for MIS

An i3 Logging Service must be present in the NGCS to collect LogEvents from NG9-1-1 Functional Elements (FEs), and to record media. These LogEvents contain unique call and incident-tracking identifiers that support a cradle-to-grave picture of calls. MIS retrieves and uses these same LogEvents for statistical analysis, and may get the events from the Logging Service or from a LogEvent Replicator. Those including MIS in RFPs should consider how it will receive the LogEvents it needs.

In transitional states, non-standard data sources for PSAP call processing analytics are required (e.g., databases, call detail records [CDRs], log files).

3.7.5.3 Information to Provide Proposers about MIS

NG9-1-1 standards are applicable to every jurisdiction. What drives the specific configuration deployed in a jurisdiction is its specific requirements. It is recommended that the information below be provided to proposers in an RFP for NG9-1-1 MIS.

1. Counts and capacities need to be identified.
    a. Number of PSAPs that represent the call handling environment.
    b. Number of interconnected ESInets (could just be one).
    c. Number of 9-1-1 voice calls needed to be handled annually. This includes calls originated on landline, wireless, VoIP, and all other networks that are mandated to provide 9-1-1 service.
    d. Anticipated voice call volume growth in the subsequent 5 to 10 years. This should include growth from an increase in the population or an increase in visitors.
2. Capacities related to the delivery of calls to the PSAPs need to be identified.
    a. Number of PSAPs or shared, hosted systems that will be supported by the MIS.
    b. Expected call volumes for each PSAP (i.e., peak loads)
    c. Number of PSAPs supported by the MIS that are fully NG9-1-1-capable, number that are IP-capable, and number that are legacy and will require LPGs.
    d. Queues in use per PSAP, if applicable, and their purpose.

3.7.5.4 Information to Request from Proposers about MIS

3.7.5.4.1 Common Metrics and Measures

When requesting any MIS, specific metrics should always be considered in order to properly measure and understand operational performance. In general, the following metrics should always be considered when looking at any MIS system: timing, volumes, bandwidth/trunk utilization, call flows, and agent activity. These high-level measures can be broken down into more discrete analytical requirements as described below. At a

minimum, metrics used for statistical measurements should conform to NENA-STA-019 [29]. Some of the reporting item examples in the following list apply only to a transitional environment.

Timing

1. Legacy and NG9-1-1 Metrics
    a. Call Taker Answer Time
    b. Caller Answer Time Experience
    c. Queue Answer Timing
    d. Average Caller in Queue Time
    e. NENA and/or National Fire Protection Association (NFPA) Answer Time Standards (are they being met)
    f. Busiest Hour(s)
    g. Most Common Emergency Service Number(s) (ESN)
    h. Highest Repeated Automatic Number Identification(s) (ANI)
2. NG9-1-1/ESInet Metrics
    a. Core Element Response Times
    b. LVF Response Timing
    c. Top Ingress IP address
    d. BCF Responses (200 OK, 600 Overload, etc.)
    e. Serviceable versus Unserviceable Calls and Percentage Delivered
    f. Number of Participants in Each Call (e.g., call conference); Call Leg Details
    g. Routing (e.g., Ingress BCF—>PSAP, Transfer PSAP—>PSAP)
    h. Initial Location Query Response Time
    i. Location Dereference Response Time
    j. Time Between Location Updates Within a Call
    k. LoST Query Response Time
    l. ALI Location Query Response Time (LPG or LSRG)
    m. Additional Data Query Response Times

Volumes

1. Legacy and NG9-1-1 Metrics
    a. 9-1-1, 10-digit Emergency and Administrative Call Type Volumes
    b. Class of Service or NG9-1-1 call type Totals
    c. Abandoned Calls
    d. Text-to- 9-1-1
    e. TDD/TTY
2. NG9-1-1/ESInet Volume Metrics
    a. ESRP Requests Processed
    b. PRF rules (e.g., how many routed by location versus ESN, diverted)
    c. LoST Update Volumes (LoST Query Volumes?)

d. All Core Element Usage Volumes
e. Payload types (media, voice, text, etc.)
f. LNG versus 100% SIP (inbound as SIP, arrival at PSAP as SIP, no analog transformations)
g. LIS/NLIS Lookup Counts (number of location requests)
h. Malformed Message Volumes
i. Incident Volumes
j. Merged Incident Volumes
k. Split Incident Volumes
l. Linked Incident Volumes
m. Reopened Incident Volumes
n. Discrepancy Report Volumes (total and per Agency)
o. "KeepAlive" Failure Volumes
p. Recording Failure Volumes
q. Transferred Call Volumes (total and per Agency)

Bandwidth/Trunk Utilization

1. Legacy Metrics
    a. Calls per Trunk
    b. Trunk Utilization
    c. Overall Circuit Utilization
    d. Overall Capacity
2. NG9-1-1/ESInet Bandwidth/Trunk Utilization (for LNG or LSRG)
    a. Percent Total Bandwidth Used (based on available bandwidth); e.g., Peak % of configured bandwidth on the data link
    b. Jitter, Packet Drop Counts, and other Quality of Service metrics
    c. Average Usage per Call
    d. Total Bandwidth Utilized

Call Flows

1. Legacy and NG9-1-1 Call Flow Metrics
    a. Call Transfers
    b. Call Conference (total duration and broken out by call leg)
2. NG9-1-1/ESInet Call Flows
    a. End-to-end Analysis (ingress to the ESInet and flow tracing to PSAP BCF, includes all elements involved and full call visibility)

Agent and Queue Activity

1. Legacy and NG9-1-1 Agent Activity Metrics
    a. Calls per Agent (9-1-1, 10-digit emergency, administrative)
    b. Agent Status (Busy, Ready, Not Ready, On Call, etc.)

c. Agent Queue Status

2. Queue Activity (NG9-1-1 and Legacy), where applicable
    a. Total Volume of Calls by Queue
    b. Average Time of Call in Queue
    c. Number of Calls Returned to Queue
    d. Number of Calls Abandoned in Queue

3.7.5.4.2 Functional Element Interface and Functional Information

NG9-1-1 Interfaces: RFPs should require proposers to describe how they will meet the requirements of *NENA i3 Standard for Next Generation 9-1-1*, NENA-STA-010 [4], by providing the interfaces below at end- state. MIS functionality in NG9-1-1 is dependent upon the LogEvents defined in NENA-STA-010. Metrics based on these LogEvents are defined in NENA-STA-019 [29].

1. Logging
    a. At least two Logging Service instances must be present to collect LogEvents per NENA-STA-010. A LogEvent Replicator (see NENA-STA-010 [4]) is recommended to support reporting and monitoring functions. Media recording functions can be allocated to Logging Service instances such that there is no single point of failure. The Logging Service must conform to the specifications given in the Logging Service section of NENA-STA-010 [4].
2. Discrepancy Reporting
    a. Per NENA-STA-010, a Discrepancy Report function is provided to notify agencies and services when any discrepancy is found. Proposers must conform to Discrepancy Reporting as specified in NENA-STA-010 [4].

NG9-1-1 Functions

A network or solution diagram that clearly maps out the end state for the ESInet and NG9-1-1 Core Services should be mandatory for all RFP responses. The functions below should be visible on the solution diagram.

1. Logging Service
    a. The MIS usage of a logging service must be presented in the solution diagram. When MIS is specifically required as part of the overall solution, proposers should describe how MIS acquires LogEvent data, and any interaction between MIS, the Logging Service, and/or a LogEvent Replicator (see NENA-STA-010 [4]).
2. Local PSAP Data
    a. The PSAP Call Handling FE is responsible for logging events related to PSAP call processing. This FE may be in the PSAP or in the serving ESInet. Proposers should describe in detail how the proposed solution supports this logging. When MIS is included in the RFP, proposers should describe how MIS

receives these events in their solution. LogEvent data flow should be shown on the solution diagram.

Call Handling MIS

The transition to NG9-1-1 will be accomplished in phases and, more often than not, a mix of NG9-1-1 PSAPs and legacy PSAPs will be present in the overall system. In order to provide PSAP-level MIS for legacy PSAPs, the functional elements below will be present at the legacy PSAP, and additional data sources will be needed to properly support the MIS system.

1. LPG
    a. An LPG provides a signaling and media interconnection point between the ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and i3 PSAPs. It should provide PIF, NIF, and LIF. An LPG logs important LogEvents that should be collected on the NGCS Logging Service. These events will support MIS analysis of call processing on the NG9-1-1 side of the gateway, with limited detail of call processing on the legacy interface. It is important that the LPG supports the required LogEvents (see NENA-STA-010 [4]), including the ALI-related events. An LPG does not log any agent events, so any collection of this type of data would not be standardized.
2. LSRG
    a. An LSRG may be supplied to provide a signaling and media connection point between a legacy selective router and an NG9-1-1 system. The LSRG should allow calls routed via a legacy selective router to terminate on an i3 PSAP, as well as allowing calls routed via an i3 ESInet to terminate to a legacy PSAP that is connected to a legacy selective router. The LSRG logs important LogEvents that can be used for MIS analysis of this call processing. It is important that the LSRG supports the required LogEvents (see NENA-STA-010 [4]), including the ALI-related events.
    b. The LSRG should also facilitate the transfer of calls to and between PSAPs that are served by legacy selective routers and PSAPs that are served by ESInets, regardless of the network from which the call originated.

3.7.5.5 PSAP Data Source

Using LogEvent data, call delivery to the LPG can be tracked. ALI queries and a limited number of call state change events on the LPG's legacy interface can also be tracked (see NENA-STA-010 [4]). Beyond that, local collection of PSAP call handling data is required. The source should be accessible either via physical connection (e.g., RS-232) or an IP connection to either a logging end point, a custom end point, or similar system to support PSAP call handling reporting.

3.7.5.6 Other Sections that Should be Reviewed

In addition to Section 3.7.5 Management Information Systems, 9-1-1 Authorities developing an RFI/RFP for Management Information Systems should also review the following sections of this document

- Human Machine Interface (HMI) (Section 3.8)
- SLAs and Other System Capacities and Performance (Section 3.10)
- Security and Cybersecurity (Section 3.11)
- References (Section 7)

3.8 Human Machine Interface (HMI)

The preceding sections outline the path a call takes from the time it is handed off to an NG9-1-1 system, and the determination of how the call should be routed and sent to an NG9-1-1 call handling system. System configurations established during system setup and current routing rules determine the call path. The system is fully automated, and typically no intervention by humans is required until the call is answered by a 9-1-1 call taker. At that point, the call handling system is there to support the 9-1-1 call taker, however, action from this point on is driven largely by a human.

While no real-time human intervention is required during the call flow, 9-1-1 Authorities require interfaces to the systems to monitor the health of the system, gather information about the performance of the system, and occasionally adjust how calls are handled. These Human Machine Interfaces are not explicitly defined in any of the standards or information documents developed by NENA Working Groups. Vendors generally make these HMIs available, but the look and feel, navigation, and other aspects are left to each vendor as a way of differentiating their services. Requirements in an RFI or RFP that reference NENA standards and information documents will not cover any HMIs. The 9-1-1 Authority issuing an RFI or RFP must define its expectations for HMIs. This can be accomplished by documenting expectations, but live demonstrations of the HMIs during the vendor selection process are essential.

3.8.1 HMIs

Vendors should make HMIs available to support the management, maintenance, monitoring, and operations of the system(s) being procured. NENA-STA-010 [4] defines the LogEventReplicator that provides real-time call processing statistics on the performance of the NGCS. NENA-STA-023 [23] requires the LogEventReplicator to provide input to the Management Console FE defined within NENA-STA-023 [23]. For example, an executive dashboard is typically required to show near-real-time status of the ESInet, NGCS, and other elements in the 9-1-1 call flow. In addition, this dashboard typically provides access to reports showing system statistics, including data to assess system performance against established SLAs.

A second set of HMIs provides tools that support the management of GIS data.

A third set of HMIs is typically available related to the PSAP CHS (Call Handling System). A Management Console provides tools and reports for the CHS, and the most important HMI supports 9-1-1 call takers as they answer a 9-1-1 call.

Finally, the MIS system, if included in the procurement, should include a set of HMIs to view, enter, and maintain MIS information.

Vendors may propose a single portal to access all of the tools outlined above, or they could propose individual portals for each tool.

3.8.2 Common Characteristics of HMIs

The standards do not prescribe the look and feel of any of the HMIs; every HMI should have a set of characteristics that the procuring agency should evaluate.

Three characteristics are required by both the published i3 standard [4] and the NG9-1-1 PSAP and ECC standard under development, NENA-STA-023 [23]:

- Single Sign-on (SSO): If a system user has access to multiple systems, a single Sign-on should be used.
- Roles based access to information via the login: Access to data and tools via the HMI should consider the roles the user has been assigned, and provide access to just those tools and data necessary for the user to perform their responsibilities.
- Security: Logins should require credentials that authenticate the user, traceable to the PSAP Credentialing Agency.

Other characteristics, not required by standards, include the following:

- Accessibility: Compliance with applicable Federal and State Laws must be a requirement. An example of this is the Web Content Accessibility Guidelines (WCAG), which are described at *WCAG 2 Overview for Web Content Accessibility Guidelines* [30]. Many states have additional accessibility requirements.
- Administrative tools that empower the 9-1-1 Authority to perform administrative functions, such as adding and deleting users and managing user roles, are strongly recommended.
- Training for all users and administrators should be evaluated for each of the HMIs.

During the proposal evaluation process, agencies should ask for a thorough demonstration of the solution's HMI, and the Agency should pay particular attention to whether the workflow(s) supported by the solution will satisfy the Agency's needs. It is also advised that the Agency describe their current workflow in detail in the RFP. The vendor could demonstrate how the workflow is supported or propose a workflow, and why.

3.8.3 Evaluation of Vendor Responses to an RFI or RFP

3.8.3.1 Use of Open-Ended Questions

Including open-ended questions like the examples below will provide one method for evaluating vendor responses. It is suggested that questions be open-ended and request screenshots of all HMIs. Examples of questions to ask may include the following:

- When call-takers log in, are calls that were already in the queue available to be answered by them?
- How does management identify individuals who should be notified when failures are detected in products, services, or networks, and what methods are available to do that notification?
- What notification methods does the system use to inform managers (or others) of important events?
- Is the HMI configurable at the Agency level?
- What are your availability standard service levels, and how is that achieved?
- In a multi-agency environment, how is each agency's secure information kept secure from other agencies?

3.8.3.2 Conducting Reference Checks

When conducting reference checks, ask for an evaluation of the HMIs provided by the vendor. Examples of questions to ask may include the following:

- How easy is it for a user to learn the HMI?
- How much training is required?
- Do the HMIs provide the necessary tools to manage the system?
- Which HMIs are available to the 9-1-1 Authority, and which ones are reserved for the vendor?

3.8.3.3 Other Considerations

It is advisable to request a demonstration of the HMIs being proposed.

3.9 Functional Elements and Services to Support Transition to NG9-1-1

The transition to NG9-1-1 must provide interoperability with legacy E9-1-1 systems. These legacy systems include OSPs that have not yet transitioned to call delivery via SIP and have not yet deployed a Location Information Server, Call transfers to and from neighboring jurisdictions that are still served by a Legacy Selective Router, and 9-1-1 call handling systems that do not fully conform to the NENA Standards. Transitional Functional Elements that provide the necessary interoperability are described below. Similarly, transitional services necessary for interoperability during the transition are also discussed.

While these Functional Elements and Services are necessary during the transition to full NG9-1-1, they reduce the functionality of an NG9-1-1 system and, at some point, will be decommissioned. Templates included in an RFP package that capture vendor pricing should acknowledge the decommissioning of these elements during the term of the contract. In addition, careful consideration should be given to deploying these elements at all. Collaborating with neighboring jurisdictions may yield options to avoid costs associated with transitional elements.

For information on NG9-1-1 PSAP/ECC transition issues, see Section 3.7.4.3 Transition Issues for NG9-1-1 PSAP/ECC.

3.9.1 Legacy Network Gateway (LNG)

LNGs are outside the ESInet (or at the edge), and calls must go through a BCF to get into or out of the ESInet. LNGs sit between the OSP's network and the NG9-1-1 system. On the ingress side, LNGs facilitate OSP call delivery over TDM networks (typically SS7) to the NG9-1-1 system. On the egress side, LNGs present the 9-1-1 call to the BCF as a full NG9-1-1 session. In some cases, current Legacy Selective Routers are used in conjunction with LNGs which can be problematic because they are aging infrastructure thus posing a resiliency risk. 9-1-1 Authorities should ensure that they know how long the LNG needs to be in place and what is being procured prior to executing an agreement with a vendor.

The FCC's Public Safety and Homeland Security Bureau issued a *Notice of Proposed Rule Making in the Matter of Facilitating Implementation of Next Generation 911 Services (NG911)* [31] that dealt primarily with the delivery of calls from a subscriber of an Originating Service Provider to an NG9-1-1 System via SIP and ultimately in full conformance to the NG9-1-1 standards. The FCC has updated Title 47, Part 9, Subpart J that sets forth requirements and conditions in order to facilitate the transition to NG 9-1-1, and to assist with creating an NG9-1-1- architecture that is secure, interoperable, and based on commonly accepted standards. These rules eliminate the need for 9-1-1 Authorities to pay for LNGs. 9-1-1 Authorities issuing an RFI/RFP for NG9-1-1 components should seek advice from their regulatory counsel. [34]

3.9.2 Legacy PSAP Gateway (LPG)

LPGs are outside the ESInet (or at the edge), and calls must go through a BCF to get into or out of the ESInet. LPGs sit between the NG9-1-1 system and a legacy PSAP call handling system. On the ingress side, LPGs facilitate the delivery of calls bound for a PSAP legacy call handling system by providing an NG9-1-1 call handling interface. On the egress side, the LPG presents the 9-1-1 call to the legacy call handling system using CAMA and provides an interface to ALI that the legacy call handling system expects.

It should be noted that LPGs are expensive and dramatically reduce the functionality available in NG9-1-1. Consideration should be given to including an optional hosted or

cloud-based Call Handling System that avoids the use of LPGs. Also note that it is likely that the rules promulgated by the FCC mentioned in the previous paragraph would not be applicable to PSAPs that require LPGs. The costs of a migration would be negatively impacted by requiring both LNGs and LPGs. Authors of RFPs should include a list of any PSAPs that may require an LPG.

3.9.3 Legacy Selective Router Gateway (LSRG)

LSRGs are outside the ESInet (or at the edge), and calls must go through a BCF to get into or out of the ESInet. LSRGs sit between an NG9-1-1 system and a legacy selective router. The side of the LSRG facing the NG9-1-1 system provides an interface that approximates another NG9-1-1 system. The side of the LSRG facing a selective router provides an interface that approximates a legacy selective router. The use of an LSRG is a potential migration path as defined in NENA-INF-008 [3]. Other migration paths are also possible.

At the time this document is being updated, some estimates suggest that 70% to 80% of the population of the United States is being served by systems transitioning to NG9-1-1. Even early-stage implementations of NG9-1-1 eliminate the legacy selective routers servicing the 9-1-1 authorities. While there are still many legacy selective routers in service, their numbers are declining rapidly. Authors of an RFP should delineate the number, type, and operators of legacy selective routers currently serving PSAPs that require call transfers. Any information about planned migrations to NG9-1-1 by these PSAPs should also be included.

3.9.4 Location Database (LDB)

The LDB is a functional replacement for the E9-1-1 ALI database. The LDB gets queried when a call is presented to the system by an OSP that does not include caller location in the PIDF-LO. The information returned from the query can be a location record provided by wireline OSPs or a pANI for VoIP and Wireless calls. The NG9-1-1 standard calls for all calls presented by OSPs to include a location object in the PIDF-LO. As OSPs implement this standard, the need for an LDB will be reduced until all OSPs conform to the standard, at which time the LDB can be eliminated. For more information on the LDB, see NENA-INF-008 [3].

3.9.5 Acceptability of Used Equipment

LNGs, LPGs, and LSRGs are all transitional elements used to bridge between the legacy E9-1-1 system and the new NG9-1-1 System. Over the term of an agreement with a vendor, any of these transitional elements deployed at the beginning of the migration may be decommissioned. As discussed in the previous section, the FCC recently promulgated rules affecting LNGs. For this reason, 9-1-1 Authorities may consider allowing the use of equipment recently decommissioned in other projects to be used as transitional elements. This could reduce project costs, however, guidelines should be established ensuring that

the equipment is still supported by the manufacturer, that updates and upgrades to the hardware and software can be made, and that all SLAs established are met. With these guidelines, especially those related to performance, availability, and Quality of Service, are met.

3.10 SLAs and Other System Capacities and Performance

A Service Level Agreement (SLA) is a commitment between the contracting authority and a service provider that outlines the details of the service, standards to which the provider will adhere, and metrics to measure the service. The SLA clearly states the level(s) of service which the contracting authority expects and the remedies to be applied if the standards are not met. SLAs are particularly common in technology environments such as NG9-1-1, and align both the issuing authority and provider expectations and responsibilities.

Generally, the following topics should be included in an SLA:

- An overview of the agreement
- Identification of all parties to the SLA
- The goals of the parties
- A description of the services being provided
- Service levels (metrics) anticipated by the parties
    - Service quality
    - Service capacity
    - Service performance
- Any services that may not be subject to the SLA or its terms
- Situations that could result in the modification, including termination, of the SLA
- A remediation plan, in the event the anticipated service levels are not met, including any anticipated maintenance and support

NENA recommends that SLA goals be clearly stated, technically achievable, able to be clearly measured, and not be cost prohibitive. Penalties for failing to meet SLA requirements should be unambiguous and substantial, but not onerous to the service provider. Where applicable, SLA requirements must extend to both the prime contractor and any subcontractors involved in service provision.

Table 3-2 Examples of Instances Where an SLA Should be Considered is not an exhaustive list, and advances in technology may result in new situations where an SLA would be appropriate or additional metrics should be considered.

Table 3-2 Examples of Instances Where an SLA Should be Considered

SLA Item	Applicability				
	ESInet	GIS	NGCS	NG PSAP	MIS
Call Path SLAs[1]					

SLA Item	Applicability				
	ESInet	GIS	NGCS	NG PSAP	MIS
Quality of Service	X		X		
Jitter	X		X	X	
Out of Order packets	X		X	X	
Lost packets	X		X	X	
Duplicate packets	X		X	X	
Mean Opinion score	X		X	X	
Total calls processed over a year	X		X	X	
Peak call volumes	X		X	X	
Maximum call setup time	X		X	X	
Average call setup time	X		X	X	
System availability	X	X	X	X	
MTTR, MTBF	X	X	X	X	
Operational SLAs					
Response times, escalation times, and level of support[2]	X	X	X	X	X
Reporting of issues not affecting service including degradation in service[2]	X	X	X	X	
Network Performance monitoring[2]	X				
Reporting on the change control process[2]	X	X	X	X	X
Notification and reporting on service level provisions[2]	X	X	X	X	
Monitoring and management of physical facilities[2]	X	X	X	X	X
Meeting requirements of ANSI/TIA-942[2]	X	X	X	X	
Process to manage and monitor system changes[2]	X	X	X	X	X
Process to monitor and manage GIS data[2]		X			
Notification and reporting to connected to the ESInet[2]	X				
Reporting on any changes and discrepancies to databases[2]	X	X	X	X	X
Backup and restore plans for databases[2]	X	X	X	X	X
Management of the network with interconnected PSAPs[2]	X				
Root cause analysis[2,3]	X	X	X	X	X
SOC monitoring and reporting[2]	X	X	X	X	X
Reporting requirements with Push To Talk Service Providers[2]					
Response times for outages by severity[3]	X	X	X	X	X
Outage escalation procedures[3]	X	X	X	X	X

SLA Item	Applicability				
	ESInet	GIS	NGCS	NG PSAP	MIS
Delivery of reports[3]	X	X	X	X	X
Allowable planned maintenance[3]	X	X	X	X	X
Change and Configuration Control[3]	X	X	X	X	X
Delivery of as-built diagram[3]	X	X	X	X	X
Specific scope of service measurement (points of demarcation)[3]	X	X	X	X	X
Vendor software development processes are in line with the Release Procedures section of NENA-INF-047.1-2025	X		X	X	
Security SLAs					
Reporting of TDoS events	X		X		
Reporting of DDoS attacks	X		X	X	
Physical security requirements	X	X	X	X	X
Vendor designs, builds, and implements their products/services in compliance with Zero Trust concepts	X		X	X	
Implementation Milestone SLAs					
Meeting project milestones	X	X	X	X	X

[1] See NENA-STA-010 [4]
[2] See NENA-STA-040 [9]
[3] See NENA-INF-047 [16]

3.11 Security and Cybersecurity

The RFP should ask cybersecurity vendors to show that they have a proactive penetration vulnerability assessment program and testing mechanisms to support it. The rationale is that having process and mitigation plans in place will assist in avoiding cybersecurity attacks that impact system health and operations.

3.11.1 PSAP Credentialing Agency and Certificate Authorities

The PSAP Credentialing Agency (PCA) is a functional element in the *NENA i3 Standard for Next Generation 9-1-1* [4] core services. It serves as the root of trust within the chain of trust in the NG9-1-1 ecosystem. It facilitates interoperability between disparate NG9-1-1 environments. The PCA establishes standardized methods for conveying identities and defining their roles within the ecosystem.

Certificate Authorities (CAs), and the infrastructure they support, form the backbone of identity assurance in NG9-1-1. CAs must be established to issue digital certificates essential

for establishing trusted communications among 9-1-1 entities and enhance the efficiency of call transfers and queries across ESInets. All digital certificates must be traceable to the root certificate for one element to authenticate another as a legitimate 9-1-1 entity. Elements without certificates traceable to the PCA will not be incorporated into the NG9-1-1 ecosystem. See NENA-STA-010 [4] for credentialing requirements.

Only valid 9-1-1 entities may operate a CA if approved by the NG9-1-1 Interoperability Oversight Commission (NIOC). Operating a CA must be done in compliance with stringent processes detailed in a Certificate Policy and Certificate Practice Statement. If a 9-1-1 entity does not wish to manage the CA, a delegated authority may be chosen to operate the CA. Authorities must contract with a competent operator to provide the service. The PCA Public Key Infrastructure (PKI) consists of a mandatory offline PCA and tier 1, and Intermediate CA (ICA at tier 2), and End-Entity Certificates at the bottom tier. Branches of the PKI may include additional tiers. It is suggested that higher level authorities, such as state or regional 9-1-1 Authorities, establish a CA. As the PCA PKI grows, Local Registration Authority(ies) may be established to provide certificates to agents. See Figure 3-2 below.

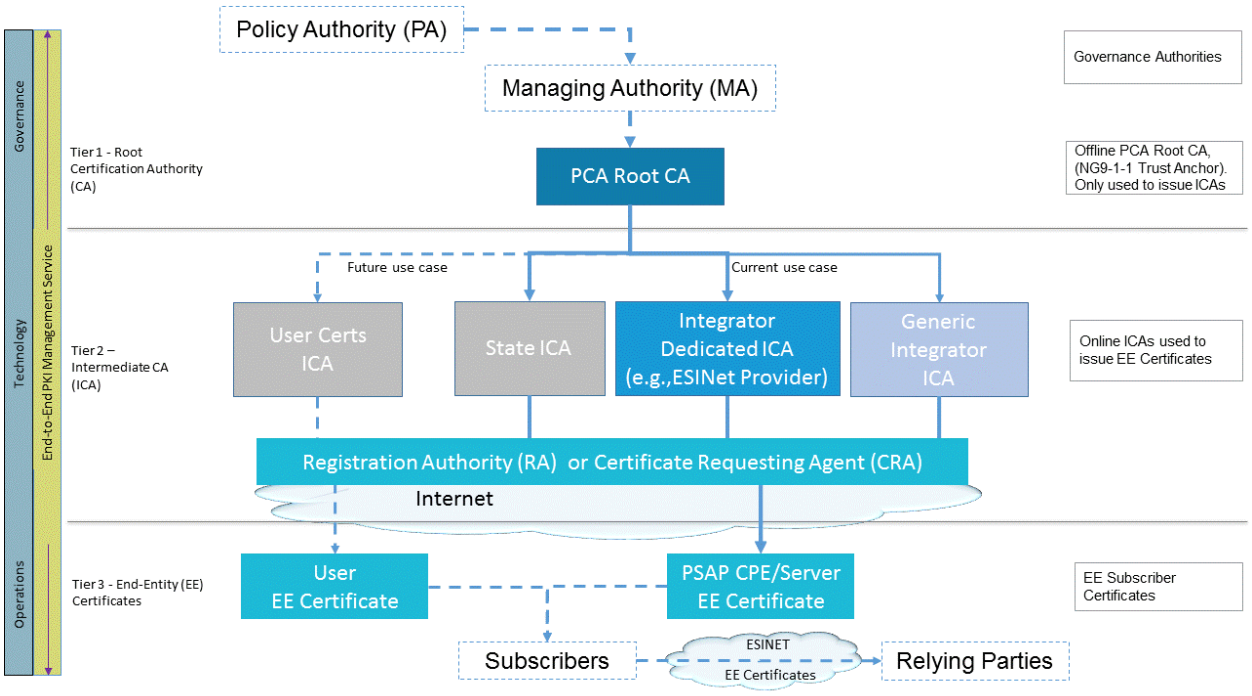

Figure 3-2 PSAP Credentialing Agency (PCA) Overview

The governance structure that represents the PKI participants is known as the Policy Authority (PA). NIOC was created by NENA and is the PA for the PSAP Credentialing Agency (PCA). The PA is responsible for identifying the appropriate set of requirements for a given community, and oversees the CAs that issue Certificates for that community. Day-to-day management of the PKI has been delegated to Eonti. The Management Authority's

primary focus is to ensure that policies for secure physical and logical Access, data sharing, and communications across the ecosystem are realized through the execution and management of the Certificate Policy (CP) requirements and its participants.

Working out exactly how the Public Key Infrastructure works is a vital component of NG9-1-11-1 deployment and must be carefully designed and implemented, with appropriate third-party audit, to assure security of the entire system. As with any security mechanism, the security of NG9-1-1 is only as good as its weakest link, and secure issuance and management of credentials is vital. An Agency applies to the appropriate certificate authority to request certificates and should contact its state or regional 9-1-1 Authority for information on the process. Certificates traceable to the PCA will have to be periodically renewed per the certificate authority's policy. Renewal will incur some expenses, and some Agency resources will be required to manage the renewal process. In addition, secure storage for the certificates and a means for securely accessing the certificates must be maintained. Methods and procedures for recovering from a "key compromise" security incident must be developed, maintained, and communicated within the Agency.

A Single Sign-On methodology must be established as part of the deployment of NG9-1-1. NENA-STA-010 [4] specifies exactly how relying parties determine whether a user is validly logged in, in what role, but does not specify exactly how the login process works. Further discussion related to HMIs necessary for provisioning, monitoring, and managing the NG9-1-1 system can be found in Section 3.8 Human Machine Interface (HMI).

4 RFP Elements

This section provides suggestions and considerations for sections that should be included in an RFP to provide adequate information to proposers to develop their response. This list is not all inclusive, nor does it address agency-specific RFP or purchasing processes or requirements.

4.1 RFP Drafting and Issuance

When drafting an RFP, the issuer should give thought to the following:

- Carefully consider agency wants/desires with realistic needs and possibilities.
- Identify needs and requirements with words such as “will,, “shall,” or “must.”
- Identify wants with words such as “optional,” “can,” and “may.”
- Decide if the selected vendor should have the fastest delivery, the lowest cost, or a combination.
- Organize the RFP with sections, subsections, introduction, requirements, selection criteria, timelines, optional items, and the process and procedures.

- Create a clear and concise RFP (longer does not necessarily mean better); ensure that it is well structured, clearly written, free of jargon, and includes a checklist of requirements.
- Evaluate your target audience:
  - Take time to pre-qualify recipients by visiting websites, interviewing principals, and requesting portfolios.
  - Send RFPs to only those companies that have a reasonable chance of doing business with your agency.
- Determine who from your organization is authorized to engage with prospective vendors.
- Identify any organizational requirements regarding the advertisement or publication of the RFP release:
  - Requirements for RFPs to be published in state Registers or Journals
  - The minimum requirements for how long/often an RFP must be advertised or published
  - Requirements for RFPs to be posted on an organization, local, or state electronic site for available opportunities
- Determine the method of issuance or release:
  - Electronic format only
  - Hardcopy only
  - Both electronic and hardcopy

4.2 Project Scope/Overview

In the project scope or overview section, include this information:

- Provide a summary of the RFP objectives, agency needs, and reasons for issuing the RFP.
- Describe the work that the agency will perform and the work the vendor will perform.
- Provide a summary of system dimensioning requirements (number of positions; number of lines; additional dependencies, such as loggers; etc.).
- Provide as much data as possible so vendors have enough information on how to structure a solution.
- Detail the minimum viable solution accepted.
- State if alternative solutions are acceptable and/or how far vendors are allowed to stray from the requirements to provide a different and potentially better solution.

4.2.1 Current System

A description of the current system should be provided to give proposers a clear picture of how the agency currently operates.

- State if there are dependencies, such as integration with a logging recorder or a radio system, which must be evaluated as part of the proposer's response.
- Consider including a high-level diagram of the current system.
- Provide as much detail as possible on the current system without infringing upon IPR boundaries.
    - Include the make and model of existing systems or equipment.
    - Include the number of existing interfaces, lines, trunks, positions, etc.
    - Include the specifications of the current network (such as bandwidth requirements, availability) or interfaces, especially for any unique or non-standard systems/equipment/interfaces.

Figure 4-1 Sample Current PSAP System Diagram is a sample diagram showing PSAP elements and interconnections. For RFPs that incorporate ESInet or NG9-1-1 Core Services, a diagram that provides details about the current 9-1-1 service infrastructure and call delivery mechanisms should be provided in the RFP.

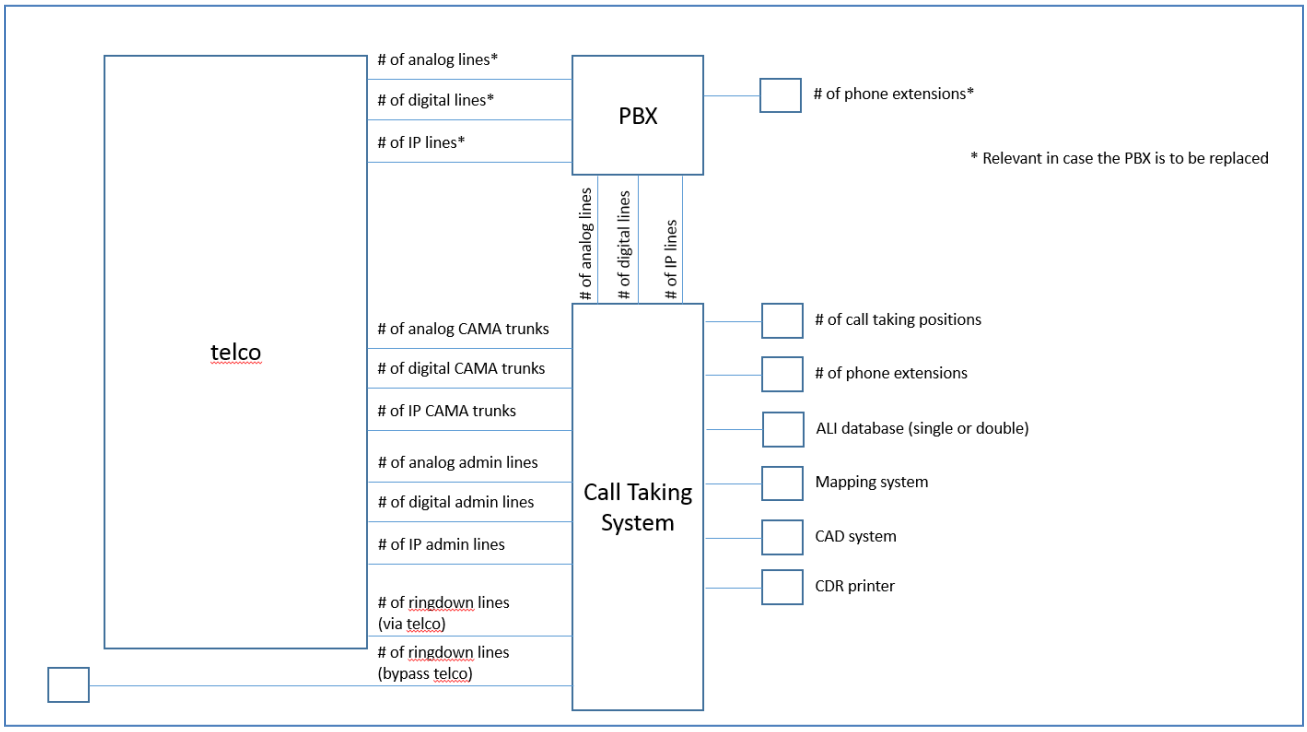

Figure 4-1 Sample Current PSAP System Diagram

4.3 Operational Environment

An explanation of the operational environment that will be responsible for interfacing with the vendor and the system should be provided in the RFP. Suggested operational considerations include the following:

- Current staffing level of the 9-1-1 Authority
  - List current positions including title, responsibilities, percentage of time available to work with the vendor, and the E9-1-1 system.
  - Provide an organizational chart to help the vendor understand the operational staff currently available to support the new system.
  - Describe the chain of command for decision-making related to the current E9-1-1 system.
- Target staffing level of the 9-1-1 Authority
  - List target positions including title, responsibilities, percentage of time available to work with the vendor, and the NG9-1-1 system.
  - Provide an organizational chart to help the vendor understand the operational staff that will be available to support the new system.
  - Describe the chain of command for decision-making related to the NG9-1-1 system.
- Proposer's recommendation on the operational staff required to properly manage the NG9-1-1 system

4.4 Schedule

A high-level schedule that includes RFP-related due dates through project completion dates post-award should be provided. Please consider any holidays or industry conferences that fall during the allotment of time given to a proposer to provide inputs (questions, proposals, presentations, etc.). A schedule may include events as shown in Table 4-1 Sample Schedule.

Table 4-1 Sample Schedule

Event	Date
RFP Release Date	Specify your dates as needed
Pre-Submission Conference	
Questions Due	
Proposals Due	Typically, 2-3 months after the Release Date
Demonstration/Oral Presentations	
Notification of Intent to Award	
Contract Signed	
Installation Begins	
Project Completed	Specify your dates as needed

4.4.1 Questions

RFPs often include a question-and-answer period in which proposers are allowed to ask questions of the agency through a defined process. The process should be detailed in the RFP, and may include the following information:

- Identify the contact for questions.
- State the preferred method for questions (e.g., e-mail, written hardcopy, telephone).
- State if addenda will be issued to provide the answers.
- State how often or when addenda will be issued.
- Ensure vendors have enough time to adjust their responses based on the answers provided.

4.4.2 Pre-Submission Conference/Site Visit

Agencies should reference the local procurement policy for requirements on determining whether a pre-submission meeting (conference) or site visit will occur. If allowable, most complex projects will benefit from pre-submission meetings.

- Determine if vendors will be required to attend a mandatory pre-submission meeting or whether the meeting is optional.
- Determine if additional information will be presented or if a site visit will be permitted.
- If screening of vendor personnel is required, provide vendors with sufficient notice of this requirement.
- The RFP should clearly state that if a pre-bid meeting is not planned, the bid may be awarded without any further notice.

4.4.3 Guidelines for Consistent Responses (Proposal Response Format)

A section on how responses are to be submitted should be included in the RFP.

4.4.3.1 Instructions to Proposers

It is recommended that you first work with your local procurement officials to identify if they have any guidelines that proposers must follow related to RFP response instructions.

Details on specific instructions may include the following:

- Electronic format or hard copy
- If hard copies, quantity requirements for binders, CDs, and thumb drives
- Page limits of responses, if any, and supporting documentation requirements (if limited, so state)
- An explanation of the rules surrounding any changes to previously submitted responses
- Shipping or email address(es) or instructions
- Point of Contact

- RFP timeline

4.4.3.2 Response Format

The response should follow the proposed format below to ensure each response is organized in the same manner for ease of review. A response format should include response and submission instructions.

4.4.3.3 Executive Summary

Key high-level decision-makers often only review an executive summary as they rely on other subject matter experts to review the proposal response in depth. An effective executive summary should demonstrate these characteristics:

- Explain how the proposer meets the needs of the agency.
- Briefly describe key elements from each proposal section.
- Be written in easy-to-understand language.
    - Do not include in-depth technical language; this section is often read by people who are not technical experts.

4.4.3.4 Company Overview/Profile

The company profile should include the following:

- Proposer's contact information
- General information about the company, including qualifications, staff, and financial stability
- References
- Identification of any subcontractors, including small businesses, minority owned businesses, or veteran owned businesses

4.4.3.5 Proposed System Description

The proposed system description should include the following:

- A detailed write-up of the proposed solution and how it meets the RFP objectives
- Diagrams

4.4.3.6 Technical Compliance Section/Matrix

The technical compliance section or matrix should include the following:

- Clear definitions as to how the response to requirements should be stated, for example:
    - Comply
    - Comply with Clarification
    - Exception
- Additional description, if needed

- A spreadsheet for the proposer to complete:
  - Agencies can "hide" scoring to be used later for point tabulation
  - Separate requirements into single line items rather than a paragraph

An example is provided below. This is an example only. PSAPs should identify acceptable options and define them.

4.4.3.6.1 EXAMPLE A

This section addresses the functional specifications set forth in the proposal. The response to the following requirements will be indicated in one of the following ways.

COMPLY	Shall be used if the proposal meets or exceeds all of the specified requirements.
COMPLY WITH CLARIFICATION	Shall be used if most, but not all of the specific requirements are met. The requirements not met must be explained in detail. If the deviation of the requirement is significant enough, it may be considered a major or minor exception.
EXCEPTION	Shall be used if the proposal does not substantially meet the specified requirements. Failure to indicate any exceptions shall be interpreted to mean that the proposer fully intends to comply with all RFP requirements as written. Explanation must be made for each item for which exception is taken, giving in detail the extent of the exception, and the reason for which it is taken. The PSAP reserves the right to give consideration or waivers for these exceptions.

Additional explanation, description, or clarification may be supplied to amplify the compliance responses. However, COMPLY WITH CLARIFICATION or EXCEPTION should require the proposers to explain why they are unable to comply or how they will meet the specifications through an exception.

4.4.3.6.2 EXAMPLE B

The same requirements listed in Example A are split into separate line items and can have their own compliance response. Proposer cannot miss a requirement, and each is scored and/or evaluated on its own.

RFP Requirement	Compliance	Explanation	Potential Weighted Scoring
The Proposer shall provide for NENA-compliant serial system interfaces for the delivery of ANI/ALI information to Computer-Aided Dispatch (CAD) and mapping applications.			*(PSAP could rank needs or assign a weighted score per requirement. Potentially hide this column from proposers and use for scoring only.)*
1. The system shall be capable of delivering ANI/ALI information to CAD and mapping applications natively via IP without a hardware or software upgrade being required.			
2. The system must also support delivery of legacy serial ANI/ALI information.			
3. The reporting interface must be capable of integrating multiple databases into one report, with the voice recordings as an attachment to the call record. ANI/ALI must be captured and stored with each 9-1-1 call, and the following items stored in their own individual database fields of appropriate size that are sortable and searchable:			
• Originating Phone Number (ANI)			
• Address or Coordinates (ALI)			
• Caller Name			
• ANI/ALI Time of Initiation			
• ANI/ALI Time of Pickup			
• ANI/ALI Time of Disconnect			
• ANI/ALI Date			
• ESN			
• Class of Service			
• Local Exchange Carrier (LEC)			

4.4.3.7 Pricing/Costs

Including a simple cost sheet will allow the agency to compare the suggested costing of the project.

- Separate costs into the categories needed for agency review, such as the following:
  - Hardware
  - Software
  - Database
  - Installation
  - Maintenance

Costs should be provided in a separate, confidential document separate from the technical proposal.

4.4.3.8 Implementation Plan/Cutover Plan

The RFP should include a request for a preliminary implementation and/or cutover plan, as well as a project timeline in the format acceptable to the PSAP.

4.4.3.9 Training Requirements

The RFP should specify the number and classification of personnel to be trained (e.g., telecommunicators, supervisors, system administrators) by type of training expected. Proposers should provide the following:

- Training Plan
- Course Descriptions
- Equipment Required
- Space/Training Room Requirements

4.4.3.10 Warranty/Service Plan Options

Proposers should provide information on the standard warranty and additional extended warranty, as well as service and maintenance plan options.

4.4.3.11 Guidelines for SLAs

SLAs establish the specific performance requirements desired by the 9-1-1 Authority. SLAs can be included in an RFP to communicate the 9-1-1 Authority's expectations. However, consider revisiting SLAs as part of contract negotiations. SLAs applicable to the components discussed have been offered for consideration in the respective sections of this document.

SLAs are specific to the component(s) of the NG9-1-1 system being purchased by a 9-1-1 Authority. For example, the required availability of an MIS is very different than that of the system that routes 9-1-1 calls in real-time. For more information, see Section 3.10 SLAs and Other System Capacities and Performance.

Some SLA-related targets have been established in NENA standards. 9-1-1 Authorities should use these values when they are available. Industry norms are being set for most other SLA targets.

To be useful, information related to the SLA must be gathered and reported to determine if the system is meeting the SLAs. "If you can't measure it, it doesn't exist."

The final contract will detail remedies if SLAs are not met. Proposed remedies can be presented in the RFP but will be finalized as part of the contract negotiations.

The 9-1-1 Authority can also define SLAs establishing the specific vendor performance requirements desired; for example, what constitutes different levels of failures, and how fast the vendor must provide a solution for the different levels of system failures.

4.4.3.12 Contract/Terms and Conditions

Proposers may seek to take exceptions, make clarifications, or provide alternatives or substitutions for consideration to the specifications of the RFP. The 9-1-1 Authority should provide clear direction with respect to how such responses must be presented in the RFP by the proposer, including a detailed explanation of the proposer's reasoning.

Contract terms and conditions statements may include the following:

- Whether or not the information submitted is considered confidential and proprietary
- Any liability to the Proposers in regard to information submitted
- Proposers submit responses at their own risk and expense

A brief description of the evaluation process may also be included.

The RFP should also clearly state that the 9-1-1 Authority will be the sole judge of the acceptability of such requests, and that its decision will be final.

4.5 The RFP Package

A sample RFP package, once it has been compiled, may consist of the following:

- Cover Letter, containing instructions to vendors
- Signature Page
- Title Page
- Table of Contents
- Schedule of Events, outlining expected timetable for procurement process
- Standard and Special Terms and Conditions
- General Information
    - Definitions of Purpose or Intent
    - Background
    - Method of Payment
    - Contract Term

    - Presentations or Demonstrations
    - Pre-Submission Meeting
    - Question and Answer Period and Contact Information
    - Deadline and Delivery Instructions, including address, phone number, and contact person
- Technical Specifications
    - Specifications (goods) or Scope of Work (services)
    - Scope of Activity (projects)
        - Project Management
        - Deliverables Schedule
        - Support, Training, or Maintenance
- SLAs
    - Level of commitment required of proposers
    - Response Time Requirements
    - Reporting Requirements
- Vendor Requirements
    - Mandatory Requirements[5]
    - Vendor Organization
    - Vendor Qualifications and Experience
    - References
    - Financials
    - Resumes
    - Sub-Contractors
- Proposal Response Format
- Cost Proposal
- Method of Evaluation and Award
    - Evaluation Criteria
    - Discussions and Best and Final Offer
    - Negotiations
- Attachments

4.6 RFP Response and Evaluation

The purpose of this section is to provide a generic checklist of response evaluation criteria, which consists of industry-standard elements commonly used to evaluate RFP responses. The detailed scoring compliance guidelines for each area of compliance for an NG9-1-1 RFP response (technical, maintenance, cost, etc.) must be fully understood and defined for

[5] Consider limiting the use of "Mandatory Response" requirements that aren't specific and clear in what they seek. Mandatory response requirements are often used to disqualify bidders; agencies should make sure these are criteria that are not going to minimize response options.

each sub-system and area of compliance as described in the relevant sections of this document.

There are a number of factors that impact RFP response evaluation and proposer selection. These factors include, but are not limited to, the following:

- Administrative rules all proposers must follow
- Elements within the proposal that are scored
- Weight or importance the 9-1-1 Authority places on each of the elements,
- Process used to score all proposals
- Staff involved
- Additional steps used to evaluate proposals after they are submitted (oral presentations, site visits, etc.)
- Scoring to be applied to these additional steps

All of these factors are involved in the procurement process up to the negotiations with the vendor(s) selected. Checklists for each of these factors can be found below.

One of the most important factors the 9-1-1 Authority must consider is how the RFP requirements are defined. Each requirement that is to be scored should have the following characteristics:

- Write RFP requirements in clear and unambiguous terms. This allows proposers to fully understand the requirement.
- Write requirements using unbiased terminology, avoiding the use of any vendors' product names or designations.
- Allow for differentiation between proposer responses. Requirements asking for "yes or no" responses are useful, but do not allow for adequate comparison of proposer responses.
- Requirements that simply refer to the standards violate items 1 and 2 above. Requirements defining what aspects of the standards are most important are very useful.
- Focus requirements on the functionality the 9-1-1 Authority requires as provided within the standard.
- Requirements that focus on functionality not defined in the standards are especially useful. As an example, operational interfaces are not documented in the standards. Requirements focused on these non-standardized aspects of an NG9-1-1 system are important.
- It is essential that all staff involved in scoring proposals clearly understand the RFP requirements.

The following is a list of possible evaluation factors germane to this topic:

- A checklist of the 9-1-1 Authority's requirements and whether the response meets the specific requirement.

- The degree to which the standard is implemented (e.g., Does the design identify the various rule types in the *NENA NG9-1-1 Policy Routing Rules Operations Guide*, NENA-INF-011.2-2020 [32]? Is there any practical limit to the number of rules that can be supported?).
- Is there an interface for the 9-1-1 Authority to enter and manage the Policy Routing Rules, or is it required to call the vendor? (e.g., What does the interface look like? Is an instruction manual provided? What expertise is required to use it? What security features are built in? What checks of the logic are included to avoid infinite loops and other issues? What reports are available?)

If the RFP in question has simply required 'Compliance with the NENA i3 standard' or some similar general statement, the issuing authority needs to consider the following issues:

- The term 'compliance' or similar is interpreted by vendors in several ways, such as 'equivalence' or 'similar to' or 'conforms with' or 'provides the same end result.' The intention in RFPs is typically to require that the proposed system actually meets the NG9-1-1 i3 standard in detail. The i3 architecture has many design points meant to support sometimes subtle, but important capabilities, beyond just the obvious routing and delivery of calls and data, as well as preparation for known near future needs.
- Vendors responding to the RFP may push agencies toward a system of the vendor's design that may not completely comply with the i3 standard.
  The meaning of their response language must be carefully inspected and evaluated.
- Vendors may believe that the 9-1-1 Authority issuing the RFP does not (yet) need certain functional capabilities for various reasons[6] and, as a result, propose a less than complete 'NG9-1-1 system' relative to the NENA NG9-1-1 i3 architectural standard.
- Does the 9-1-1 Authority desire some form of guarantee that the vendor will provide components in reasonable timeframes and at reasonable cost in the future?

A recommendation has been made that a working group be created to more fully provide guidance on all factors of proposer evaluation and selection. The sections below provide a checklist of considerations.

4.6.1 Response Evaluation Considerations

Evaluation steps generally include the following:

1. Establish the RFP Evaluation Committee

[6] Such as lack of IP interfaces from originating service providers, or because the vendors believe that Policy Routing can be replaced by some other internal vendor-managed process that only supports overflow and alternate routing rather than the full capability of the i3 Policy Routing Function.

   a. All evaluators should be familiar with the RFP document, and all agency-specific documentation is signed or completed prior to evaluation (such as a non-disclosure agreement)
2. Evaluate technical proposals
3. Evaluate cost proposals
4. Conduct oral interviews and/or demonstrations
5. Re-evaluate based upon steps 2, 3, and 4
6. Enter into negotiations
7. Final recommendation for award according to agency- or state-specific guidelines and regulations

4.6.2 Evaluation and Scoring

Considerations for scoring should include the following:

- Proposer's checklist (to determine if all required documentation has been submitted)
- A breakdown of how scoring will be weighted

Technical Compliance	XX% or # of Points
Maintenance and Support	XX% or # of Points
Total System Cost	XX% or # of Points
Vendor Experience and Capability	XX% or # of Points
Demonstrations or Oral Presentations	XX% or # of Points
Total	**XXX% or ## of Points**

4.6.3 Demonstrations or Oral Presentations

If a need is determined at any time for a demonstration or oral presentation, agencies may wish to provide the following information to proposers:

- Amount of time available for set up
- Amount of time available to present
- Need for a live system required or if demonstration software/system is sufficient

4.6.4 Agency-Specific Requirements

Agency-specific (or city, county, state) requirements may include the following:

- Insurance Requirements
- Bid Bond
- Performance Bond
- Terms and Conditions/Sample Contract
- Minority-owned/Women-owned/Veteran-owned, etc. requirements
- Penalty Fees

4.6.5 Logistics Summary

In summary, the logistics behind drafting, developing evaluation standards, and RFP issuance can require as much effort and input from agency staff as development of the technical requirements. When the agency provides a clear, concise RFP with specific instructions to proposers, the agency will have a higher probability of receiving proposal responses that are easier to evaluate and easier to compare. The agency then will ultimately be able to choose the best equipment or service to meet its needs.

5 Impacts and Considerations

5.1 NG9-1-1 Operations Impacts Summary

Deciding exactly what resources will be shared and how the work of PSAPs will utilize the shared resources has important implications for exactly how the public's need for 9-1-1 service will be met.

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, the administration and management of several functions require a number of central 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 the following:

- Administration and management of inbound Border Control Function (BCF) assignments, including determination of what Originating Service Provider (OSP) entities are providing calls/messages and data on which logical input points.
- Coordination, resolution, and management of Geographical Information System (GIS) data feeds from individual PSAPs or local source points, including resolution of gaps and overlaps, and measuring GIS accuracy overall.
- Coordination and management of Location Validation Function (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 OSP entities or a third-party provider to OSP entities. In any case, the 9-1-1 Authority with responsibility for NG9-1-1 Core Service operations has the responsibility to see that the process works effectively.
- Management of other databases that control various Core Services functional elements and their processing functions.
- 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 Telecommunicator positions) based on type of call (text or video). The design of the i3 architecture also includes the Policy Routing Function (PRF) automatically sensing PSAP delivery channel or PSAP equipment status, with the appropriate i3 compliant software at the PSAP, and making pre-defined changes in call routing.

- Logging and alarm messaging in the NG9-1-1 Core Services system will need to be managed, reacted to, and resolved.
- Administration and authorization of functional elements that subscribe to, and notify subscribers of, events. This is especially important for entities outside the core that wish to participate, such as trauma centers and public works departments.
- If digital certificates are used, administration is required.

5.2 Operations Impacts Summary

Evolving to NG9-1-1 has wide-ranging operational impacts, and implementing this document may have an influence on various stakeholders at the PSAP. Many times, the RFP process includes managing personnel not typically assigned to procurement duties. Areas of impact one may consider in the implementation of this document include, but are not restricted to, the following:

- Identification of personnel who may be part of the RFP development process, evaluation, and review activities
- Analyzing the impact on their existing responsibilities
- Reviewing their current schedule
- Understanding the potential need for overtime

5.3 Technical Impacts Summary

Evolving to NG9-1-1 has wide-ranging technical impacts on stakeholders at the PSAP with the potential delivery of new technology. Implementing the advice given in this document is expected to impact the technical specifications contained in NG9-1-1 RFPs, and to similarly impact the resulting implementation of systems and services, and the implementation of infrastructure for monitoring and managing those systems and services.

5.4 Security Impacts Summary

Evolving to NG9-1-1 has wide-ranging security impacts on stakeholders at the PSAP with the potential delivery of new technology. The impacts of the implementation of this document are both direct and indirect.

Direct impacts to consider during the implementation of this document in relationship to the RFP process include, but are not limited to:

- Physical access to the PSAP
- Information on the PSAP infrastructure

- Design and implementation of infrastructure to monitor and manage the security of facilities, systems, and services
- Sharing of information that may fall under Intellectual Property Rights (IPR)

Therefore, stakeholders at the PSAP should review any and all security processes and procedures for the agency during the RFP process, and implement the security specifications contained in the documents included in Section 7 References.

5.5 Recommendation for Additional Development Work

There are several topics that are not currently, but near-term, may be important considerations in RFPs and RFIs. The topics listed below are those that are known to the working group today, but all require further development before they are addressed in a subsequent version of this document. The time frame in which these topics become mature varies, but all should be monitored. Note that some or all of these topics may warrant a separate NENA document that this document can reference, but some may be addressed in a subsequent version of the document.

1. *Rollout of the NG9-1-1 test program is currently being developed by the NG9-1-1 Interoperability Task Force*: In Section 3.4 Value of Standards above, a brief description of the NG9-1-1 Interoperability Task Force is provided. If the program is launched, it will have a profound impact on RFIs and RFPs issued by 9-1-1 Authorities.
2. *PCA business options*: An overview of PCAs is provided above in Section 3.11.1 PSAP Credentialing Agency and Certificate Authorities, along with considerations a 9-1-1 Authority may want to include in an RFI or RFP. Not covered in that section are the options for assigning roles and responsibilities to stakeholder groups within the 9-1-1 Authority and external to the 9-1-1 Authority.
3. *Artificial Intelligence (AI)*: The current application of AI focuses on how to handle non-emergency calls, report transcription, and other administrative and repetitive activities undertaken by PSAP staff. Use of AI in the processing of 9-1-1 calls is currently rare. However, as the technology improves and PSAP staff becomes more comfortable with the technology, it will likely be deployed more widely in public safety both at the PSAP and in NGCS.
4. *FCC regulations*: On a continuing basis, the FCC will be promulgating new regulations that may affect the content found in RFIs and RFPs.

5.6 Anticipated Timeline

The implementation of this document can be undertaken immediately. The guidelines contained in this document can be applied by anyone preparing RFPs at any stage in their process. Best results may be realized if the recommendations and guidelines are applied at the beginning of the process.

5.7 Cost Factors

The contents of this document propose considerations that will help avoid unnecessary costs and work effort associated with RFP creation, analysis, issuance, and award process for an NG9-1-1 procurement.

The guidelines may serve to reduce RFP development costs since they provide a procurement baseline. In addition, this document will help teams that are charged with developing an RFP to understand and plan for the following:

- The full extent of the effort
- The skills and knowledge required
- The depth of research required

Potential cost savings include, but are not limited to, the following:

- The cost of responding to vendor questions related to information missing or unclear in the RFP
- The cost of missing information that may require costly change orders once a contract is signed
- The cost of retracting an incomplete or inaccurate RFP
- The cost of reissuing an RFP due to a lack of qualified responses to an incomplete or unclear initial RFP

A 9-1-1 Authority should understand that there will be a cost to both the PSAP and the proposers in the preparation of an RFP, and it may vary depending on the type of approach taken to generate the RFP.

Three common approaches to RFP creation, analysis, issuance, development, and award process include, but are not restricted to, the following:

1. Prepare the RFP internally: With this approach, the 9-1-1 Authority designates internal staff to create the RFP. The costs associated with this approach may include a calculation focused on the number of hours projected by staff to research, create, and review the RFP. Taking this approach, the 9-1-1 Authority should determine if they have subject matter expertise on staff qualified to create the content for the RFP; if the expertise is not inherent, time will be needed by staff to research the subject which could increase time and cost to complete.
2. Partner with another 9-1-1 Authority or agency: This approach is similar to preparing the RFP internally, but the 9-1-1 Authority identifies a nearby agency or agencies that are considering the same type of procurement. The involved agencies may realize a reduced cost burden by forming a team consisting of members from each agency to prepare the RFP. Taking this approach, the 9-1-1 Authority may be able to leverage the subject matter expertise offered by a nearby agency. Once

collaboration is complete, the agencies can do a combined procurement for a shared system or may each elect to release the RFP as stand-alone entities.

3. Engage a third party: Using this approach, the 9-1-1 Authority identifies a qualified external third-party that already has subject matter expertise in the area of procurement sought. In this model, a larger portion of the cost is transferred to the third party. In taking this approach, the 9-1-1 Authority should anticipate there will still be involvement from internal staff for initial input on the procurement scope, in addition to review and approval cycles for the RFP. Ultimately, the RFP is still owned by the issuing agency so they must understand the RFP requirements and general content. If using this method, the 9-1-1 Authority should work with the selected third party to establish the level of effort for internal staff.

5.8 Cost Recovery Considerations

The contents of this document propose considerations that will help avoid unnecessary costs and the work effort associated with RFP creation, analysis, issuance, and the award process for an NG9-1-1 procurement.

Therefore, normal business practices shall be assumed, and RFP development costs are normally borne by the agency issuing the RFP. Cost recovery may be available in some jurisdictions via grants or through the use of surcharge funds, if authorized as an eligible expense.

5.9 Additional Impacts (non-cost related)

The content of this document, in conjunction with other NG9-1-1 material, will assist in establishing a smooth, timely, and efficient RFP for the implementation of NG9-1-1. Therefore, additional impacts are not anticipated by this authoring group.

6 Abbreviations, Terms, and Definitions

See the NENA Knowledge Base (NENAkb) [1] for a Glossary of terms and abbreviations used in NENA documents. Abbreviations and terms used in this document are listed below with their definitions.

Term or Abbreviation (Expansion)	Definition / Description
9-1-1 Authority	A State, Provincial, Territorial, County, Regional, or other governmental entity responsible for 9-1-1 service operations. For example, this could be a county/parish, Indigenous or other local government, a special 9-1-1 or Emergency Communications District, a Council of Governments, or other similar body.

Term or Abbreviation (Expansion)	Definition / Description
AS (Autonomous System)	An Autonomous System is a collection of one or more associated Internet Protocol (IP) prefixes with a clearly defined routing policy that governs how the AS exchanges routing information with other Autonomous Systems. **Related Terms:** ASN (Autonomous System Number)
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.
CDR (Call Detail Record)	A record stored in a database recording the details of a received or transmitted call. The data information sent to the ALI computer by a remote identifying device (PBX, Call Position Identifier, etc.).
CHS (Call Handling System)	A communications software system and equipment used to receive and process Calls.
CSP (Communications Service Provider)	This term is used generically to refer to any and all providers of telecommunications services that may be used to generate a 9-1-1 call, and who would interconnect in any fashion to the 9-1-1 network. CSPs include wireline local exchange carriers, Wireless Service Providers, VoIP Service Providers, operators of large PBXs and any other entity providing telecommunications services.
DDoS (Distributed Denial of Service Attack)	A form of DoS in which the attack source is more than one, often thousands of, unique IP addresses. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.
DNS (Domain Name System)	A global, distributed, delegated database of records about domain names. Each type of record holds a specific type of information. DNS is queried with a domain name and desired record type. The response is the record data associated with the queried data. Some records contain an IP address for a domain name, other record types contain email or SIP server information for a domain name, etc.

Term or Abbreviation (Expansion)	Definition / Description
ECC (Emergency Communications Center	A facility designated to receive and process requests for emergency assistance, which may include 9-1-1 calls, determine the appropriate emergency response based on available resources, and coordinate the emergency response according to a specific operational policy. Note: The term "ECC" does not have the same meaning as "PSAP."
ECRF (Emergency Call Routing Function)	A functional element in NGCS (Next Generation Core Services) which is a LoST (Location-to-Service Translation) 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.
EIDO (Emergency Incident Data Object)	A JSON-based (JavaScript Object Notation) object that is used to share emergency incident information between and among authorized entities and systems. NENA has adopted the JSON-based EIDO for sharing incident information among authorized NG9-1-1 entities and systems.
E9-1-1 (Enhanced 9-1-1)	E9-1-1 (Enhanced 9-1-1) is a telephone system that includes network switching, database(s), and Public Safety Answering Point premises 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.

Term or Abbreviation (Expansion)	Definition / Description
ESInet (Emergency Services IP Network)	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 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 NGCS (Next Generation 9 1 1 Core Services).
ESN (Emergency Service Number)	A 3–5 digit number that represents one or more ESZs (Emergency Service Zone), stored as a 3-5 character numeric string in a GIS database. An ESN is defined as one of two types: Administrative ESN and Routing ESN.
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.
ESZ (Emergency Service Zone)	A geographical area that represents a unique combination of emergency service agencies (e.g., Law Enforcement, Fire, and Emergency Medical Service) that are within a specified 9-1-1 governing authority's jurisdiction. An ESZ can be represented by an Emergency Service Number (ESN) to identify the ESZ.
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. Also known as: Functional Entity
GIS (Geographic Information System)	A system for capturing, storing, displaying, analyzing, and managing data and associated attributes which are spatially referenced.

Term or Abbreviation (Expansion)	Definition / Description
GUI (Graphical User Interface)	A form of user interface that allows users to interact with electronic devices through graphical icons and audio indicators, such as primary notation, instead of text-based user interfaces, typed command labels, or text navigation.
HMI (Human Machine Interface)	The means through which a person interacts with an automated system/machine. A vehicle or an installation is sometimes referred to as the human-machine interface.
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.
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).
IVR (Interactive Voice Response)	A technology that allows a computer to interact with humans, where a person can hear a computer-generated voice and respond by speaking or generating DTMF tones on a keypad. As an example, a "Ported Number IVR" is a computer system accessible by registered users, utilized to identify the Service Provider and 24 X 7 access number for telephone numbers that have been ported or pooled.
LDB (Location Database)	A server that retains all of the current information, functionality, and interfaces of today's ALI and can utilize the new protocols required in an NG9-1-1 deployment.

Term or Abbreviation (Expansion)	Definition / Description
LIF (Location Interworking 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. In an ingress LSRG, this functional component interacts with an ALI system as if it were a PSAP to acquire location that can be used to route the emergency call and to provide location information to the PSAP. In an egress LSRG, an ALI system will interact with this functional component as if it were an MPC/GMLC to obtain location information.
LIS (Location Information Server)	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 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 Media Access Control (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 a non-IP originating network and a Next Generation Core Services (NGCS) enabled network.
LoST (Location-to-Service Translation Protocol)	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.

Term or Abbreviation (Expansion)	Definition / Description
LPG (Legacy PSAP Gateway)	A signaling and media interconnection point between an ESInet and a legacy PSAP. It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and NG9-1-1 PSAPs. The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router and a legacy PSAP) on the other.
LSRG (Legacy Selective Router Gateway)	Provides an interface between a 9-1-1 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 (Next Generation 9-1-1 Core Services) 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 is adequate and specific enough to direct responders to the right location.
MIS (Management Information System)	A computer system that collects, stores, and correlates data from multiple systems and allows users to readily access data to support operational and strategic decision making on performance, trends, traffic capacities, etc.
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.

Term or Abbreviation (Expansion)	Definition / Description
NG9-1-1 (Next Generation 9-1-1)	An IP-based system comprised of hardware, software, data, and operational policies and procedures that: (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities; (E) supports data or video communications needs for coordinated incident response and management.
NIF (NG9-1-1 Interworking Function)	The functional component of a Legacy Network Gateway, Legacy PSAP Gateway, or Legacy Selective Router Gateway that provides NG9-1-1 specific processing of the call that is not provided by an off-the-shelf protocol interwork gateway.
PBX (Private Branch Exchange)	A private telephone switch that is connected to the Public Switched Telephone Network.
PIDF-LO (Presence Information Data Format–Location Object)	An extension to PIDF that contains location information.
PIF (Protocol Interworking Function)	The functional component of a Legacy Network Gateway, Legacy PSAP Gateway, or Legacy Selective Router Gateway that interworks legacy PSTN signaling such as ISUP or CAMA with SIP signaling.
POI (Point of Interconnection)	A Physical Demarcation between an originating carrier network and an NG9-1-1 network.
PSAP (Public Safety Answering Point)	A physical or virtual entity where 9-1-1 calls are delivered by the 9-1-1 Service Provider.
QoS (Quality of Service)	As related to data transmission, a measurement of latency, packet loss, and jitter.
RFI (Request for Information)	A customer document used at an early stage of a procurement to create a list of viable bidders who will later be invited to render an offer or respond to an RFP.

Term or Abbreviation (Expansion)	Definition / Description
RFP (Request for Proposal)	A standardized document for requesting negotiated bids. In more general terms, it is an announcement from a customer or funding source that is seeking proposals for a specific program, project, or work effort.
RFQ (Request for Quote)	A document prepared by a buyer defining his needs for service or equipment in fairly broad terms and sent to one or several vendors. The RFQ is much less detailed than the RFP.
SBC (Session Border Controller)	A commonly available functional element that provides security, NAT (Network Address Translation) traversal, protocol repair, and other functions to VoIP signaling, such as SIP. A component of a Border Control Function.
SI (Spatial Interface)	A standardized interface between the GIS data and the functional elements that consume GIS data, such as the ECRF, LVF, and Mapping Data Service.
SIP (Session Initiation Protocol)	A protocol specified by the IETF (RFC 3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, NENA i2, and NENA i3.
SLA (Service Level Agreement)	A contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.
SOI (Service Order Input)	A file of completed service order updates that is sent to the DBMSP (Data Base Management System Provider) by all Service Providers.
TDoS (Telephony Denial of Service)	A form of DoS directed at a telephony interface that generates numerous phone calls, tying up the network and preventing the destination from receiving legitimate calls. Occasionally, the "T" in TDoS may be shown as Telephone or Telecommunications.
TVSS (Transient Voltage Surge Suppressor)	Devices designed to protect critical PSAP equipment from transients induced on powering and data/signal/telecommunications conductors.

Term or Abbreviation (Expansion)	Definition / Description
URI (Uniform Resource Identifier)	An identifier consisting of a sequence of characters matching the syntax rule that is named <URI> in RFC 3986. It enables uniform identification of resources via a set of naming schemes. A URI can be further classified as a locator, a name, or both. The term "Uniform Resource Locator" (URL) refers to the subset of URIs that, in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network "location"). The term "Uniform Resource Name" (URN) has been used historically to refer to both URIs under the "urn" scheme [RFC 2141], which are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable, and to any other URI with the properties of a name. An example of a URI that is neither a URL nor a URN is sip:psap@example.com.

7 References

[1] National Emergency Number Association. "NENA Knowledge Base Glossary." Updated May 6, 2025. https://kb.nena.org/wiki/Category:Glossary.

[2] Spectrum Auction Reauthorization Act of 2023. H.R. 3565, 118th Cong. (2023).

[3] National Emergency Number Association. *NENA NG9-1-1 Transition Plan Considerations Information Document.* NENA-INF-008.2-2013. Alexandria, VA: NENA, approved November 20, 2013.

[4] National Emergency Number Association. *NENA i3 Standard for Next Generation 9-1-1.* NENA-STA-010.3-2021. Alexandria, VA: NENA, approved July 12, 2021.

[5] National Emergency Number Association. "NG9-1-1 Industry Collaboration Events (ICE)." Accessed September 9, 2025. https://www.nena.org/page/ng911_ice.

[6] NG9-1-1 Interoperability Task Force. "NG9-1-1 Interoperability Task Force." Accessed September 9, 2025. https://ng911interop.org.

[7] National Emergency Number Association. *NENA Emergency Services IP Network Design (ESIND) Information Document.* NENA-INF-016.2-2018 (originally 08-506). Alexandria, VA: NENA, approved April 5, 2018.

[8] Internet Engineering Task Force. Network Working Group. *An Architecture for Differentiated Services*. S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. RFC 2475, December 1998.

[9] National Emergency Number Association. *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*. NENA-STA-040.2-2024. Alexandria, VA: NENA, approved October 28, 2024.
[10] National Emergency Number Association. *NENA Security Audit Checklist*. NENA-REF-012.1-2025. Alexandria, VA: NENA, approved May 6, 2025.
[11] National Institute of Standards and Technology. "Innovation Lab." Accessed September 9, 2025. https://www.nist.gov/ctl/pscr/research-portfolios/innovation-lab.
[12] Center for Internet Security. "CIS Critical Security Controls." Accessed September 9, 2025. https://www.cisecurity.org/controls.
[13] U.S. Department of Homeland Security. "Homeland Security." Accessed September 9, 2025. https://www.dhs.gov.
[14] Federal Communications Commission. *Radio Frequency Devices*. 47 C.F.R. Part 15. Last amended September 8, 2025.
[15] Federal Communications Commission. *Resiliency, Redundancy and Reliability of Communications*. 47 C.F.R. Part 12 (Jan. 5, 2020).
[16] National Emergency Number Association. *NENA NG9-1-1 Operational Diversity and Redundancy Information Document*. NENA-INF-047.1-2025. Alexandria, VA: NENA, approved April 28, 2025.
[17] National Emergency Number Association. *NENA Information Document for GIS Data Stewardship for Next Generation 9-1-1 (NG9-1-1)*. NENA-INF-028.2-2023. Alexandria, VA: NENA, approved September 20, 2023.
[18] National Emergency Number Association. *NENA Standard for NG9-1-1 GIS Data Model*. NENA-STA-006.2-2022. Alexandria, VA: NENA, approved September 21, 2022.
[19] National Emergency Number Association. *NENA Information Document for Development of Site/Structure Address Point GIS Data for 9-1-1*. NENA-INF-014.1-2015. Alexandria, VA: NENA, approved September 18, 2015.
[20] National Emergency Number Association. *NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF-US) Standard*. NENA-STA-004.2-2024. Alexandria, VA: NENA, approved February 25, 2024.
[21] National Emergency Number Association. *NENA Demarcation Points in NG9-1-1 Information Document*. NENA-INF-003.2-2024. Alexandria, VA: NENA, approved May 22, 2024.
[22] National Emergency Number Association. *NENA Standard for Emergency Incident Data Object (EIDO)*. NENA-STA-021.1-2021. Alexandria, VA: NENA, approved October 14, 2021.
[23] National Emergency Number Association. *NENA NG9-1-1 PSAP and ECC Specifications for the NENA i3 Solution*. NENA-STA-023.1-202Y. Alexandria, VA: NENA (forthcoming).
[24] National Emergency Number Association. *NENA Standard for the Conveyance of Emergency Incident Data Objects (EIDOs) between Next Generation (NG9-1-1)*

Systems and Applications. NENA-STA-024.1.1-2025. Alexandria, VA: NENA, approved January 16, 2025.

[25] National Emergency Number Association. *NENA Transition to i3 PSAP Standard*. NENA-STA-049.1-202Y. Alexandria, VA: NENA (forthcoming).

[26] Federal Bureau of Investigation. "Law Enforcement Online." Accessed September 9, 2025. https://archives.fbi.gov/archives/news/stories/2005/september/leo080605.

[27] Federal Bureau of Investigation. "National Crime Information Center (NCIC)." Accessed September 9, 2025. https://irp.fas.org/agency/doj/fbi/is/ncic.htm.

[28] Federal Bureau of Investigation. "CJIS Security Policy." Accessed September 9, 2025. https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center.

[29] National Emergency Number Association. *NENA NG9-1-1 Call Processing Metrics Standard*. NENA-STA-019.2-2022. Alexandria, VA: NENA, approved September 21, 2022.

[30] World Wide Web Consortium (W3C). *WCAG 2 Overview for Web Content Accessibility Guidelines (WCAG)*. https://www.w3.org/WAI/standards-guidelines/wcag/, May 6, 2025.

[31] National Emergency Number Association. *NENA NG9-1-1 Policy Routing Rules Operations Guide*. NENA-INF-011.2-2020. Alexandria, VA: NENA, approved June 18, 2020.

[32] Federal Communications Commission. "Next Generation 911" C.F.R. 47, Part 9, Subpart J (09-29-2025).

8 Appendix A—Suggested Steps in the NG9-1-1 Procurement Process

1. Needs Assessment

Conduct a needs assessment to build consensus among stakeholders.

a. Define stakeholder needs such as call handling system capabilities (i.e., text, video, location-based routing), interoperability, reliability, and redundancy.

2. Current Conditions

Evaluate current conditions:

a. Review each PSAP/dispatch center's unique conditions related to the implementation of NG9-1-1 service.
b. Review available infrastructure that could support the implementation of NG9-1-1 service.
c. Review statutory and regulatory frameworks.

3. Gap Analysis

Conduct a gap analysis that assesses the performance of the current system to determine if current objectives are being met and, if not, what steps should be taken to meet them. This includes, but is not limited to, the following:

a. Evaluate the existing call handling system capability.
b. Review CAD, GIS, and RMS compatibility with NG9-1-1.
c. Assess the need to process multimedia data.
d. Identify potential cybersecurity vulnerabilities.
e. Determine staffing and training needs.
f. Estimate costs for required system upgrades.
g. Identify potential grant funding sources.
h. Perform a comprehensive assessment using a structured framework such as the NENA NG9-1-1 Readiness Checklist.
i. Compare the current state with the desired NG9-1-1 capabilities to identify deficiencies.

4. Current Standards

Review current national and state/provincial standards and regulations. This should include a review of the following documents:

a. NENA NG911 Standards, Requirements Documents, and Information Documents, including works in progress
b. FCC or CRTC NG9-1-1 regulations and reports

5. Stakeholder Requirements

Work with all stakeholders to ensure all requirements identified in the Gap Analysis are included in RFP proposals.

a. Engage all internal and external partners to determine who will be impacted by NG9-1-1.
b. Define, document, categorize, and rank all key requirements.

6. Procurement

Work with state/provincial/local procurement officials to ensure compliance with established processes.

a. Provide a general project overview and discuss objectives.
b. Review technical and functional requirements.
c. Set deadlines.

7. Issue RFP

a. Provide clear instructions on the process, format, criteria, and deadlines.
b. Receive and acknowledge proposals.
c. Verify compliance.
d. Respond to vendor questions.

8. Scoring Matrix

a. Create evaluation criteria based on requirements, cost, security, resilience, and vendor capability.

9. Vendor Selection

a. Evaluate proposals.
b. Score and rank proposals.
c. Shortlist vendors.
d. Conduct interviews or presentations.

10. Contract Negotiations

a. Negotiate terms with specific deliverables, timelines, and price.
b. Determine payment schedule, including penalties for non-performance.

11. Implementation

a. Develop an implementation roadmap with specific timelines.
b. Launch project.

12. System Sustainability

a. Engage partners to review the system (6-12 months) after go-live.
b. Identify gaps.
c. Resolve issues.

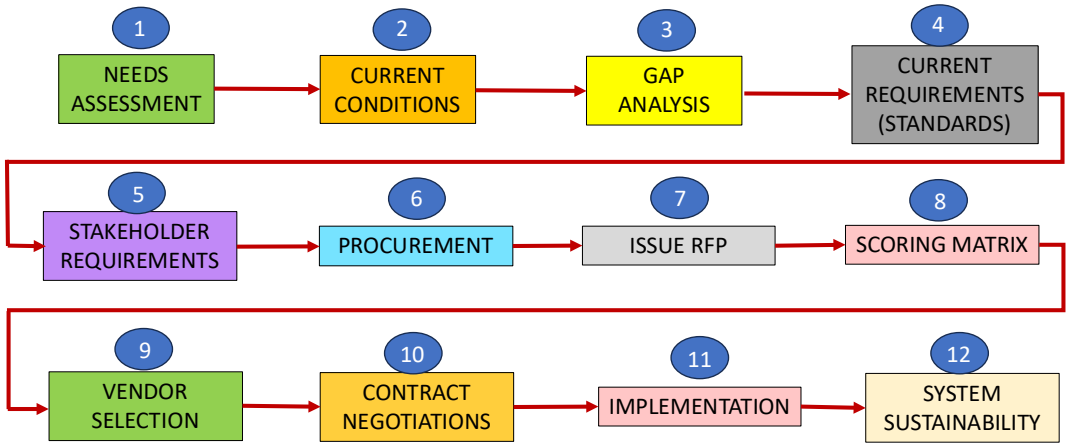

Figure 8-1 Suggested Steps in the NG9-1-1 Procurement Process

Acknowledgements

The National Emergency Number Association (NENA) PSAP Logistics Committee, RFP Working Group developed this document.

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Diane Harris, ENP PSAP Logistics Committee Co-Chair	Zetron, Inc
Amy McDowell, ENP PSAP Logistics Committee Co-Chair	Greenville County South Carolina
Sandi Stroud, ENP, Co-Chair	1Spatial, Inc
Ray Paddock, Co-Chair	Synergem Technologies, Inc
Tom Breen, EP Document Editor	SecuLore, an Exacom company
Jane Brueckner, ENP Notes Manager	Mission Critical Partners
Bob Finney III, ENP	Collier County Sheriff Office, FL
Budge Currier, ENP	Emergency Technology Consulting
Craig S. Breneiser, ENP	Essential Management Solutions, LLC
Eric Parry, ENP	Criterion Consulting Services
Jay Slater, ENP	Bandwidth
Max Iwaniec	Comtech/Allerium
Michael Smith	Equature/DSS Corp.
Steve McMurrer, ENP	Fairfax County, VA

Special Acknowledgements:

NENA's Committee Resource Management Team has facilitated the production of this document through the prescribed approval process.

The RFP Working Group is part of the NENA Development Group that is led by:

- Wendi Rooney, ENP, and Lisa Dodson, ENP, Development Steering Council Co-Chairs
- Brandon Abley, ENP, Chief Technology Officer
- April Heinze, ENP, VP, Chief of 9-1-1 Operations