Forest Guide Request for Proposals

Approved 18 November 2020
by the NG9-1-1 Interoperability Oversight Commission (NIOC)

Overview

Respondents (“proposers” and/or CONTRACTOR) to this RFP are being asked to provide the services meeting the Statement of Work and tasks associated with being the national Forest Guide (FG) operator, in cooperation with NENA, for the Next Generation 9-1-1 (NG9-1-1) system. The successful respondent to this RFP will be responsible for configuring, deploying, operating, and making available to FG users a national FG cluster, on behalf of NENA, through the NIOC. The NIOC will establish the process for awarding the FG contract to the FG operator and the NIOC will also provide governance, oversight, and policy directives to the FG operator throughout the life of the resulting contract.

The NIOC expects the FG operator to:

- Accept authoritative Emergency Services Routing Function (ECRF)/Location-to-Service Translation (LoST) server information from appropriate emergency services authorities that have responsibility for ECRF/LoST trees at:
  - State, territory, national (e.g., non-U.S. countries),
  - other levels (e.g., county or regional levels in states lacking a statewide ECRF/LoST tree),
- Implement a sustainable, revenue-neutral funding model through the NIOC
- Provide a non-real-time LoST-sync/discovery service for provisioning of top-level LoST geospatial routing information. This service SHALL allow for provisioning of a local replica of FG information. The incumbent will be required to explain how this discovery service will be interoperable with FGs outside of the United States, particularly in Canada.

Finally, there are a number of optional parameters that are not required, but strongly desired, to be proposed by responders, including:

- A preference for open-source software
- Provision of LoST-as-a-Service
- LoST/FG Test Service
- Integration with NENA Enhanced PSAP Registry and Census (EPRC)

Normative Language

The form of emphasis (UPPER CASE) shall be consistent and exclusive throughout the document. Any of these words used in lower case and not emphasized do not have special significance beyond normal usage.

MUST, SHALL, REQUIRED: These terms mean that the definition is a normative (absolute) requirement of the specification.

MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option "must" be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option "MUST" be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

Proposers that cannot fulfill the terms of an optional requirement must justify why their offering cannot comply with the optional requirement.

These definitions are based on IETF RFC 2119.[1]

Background

About NIOC

The NG9-1-1 Interoperability Oversight Commission (NIOC) is the independent oversight governance body for the NG9-1-1 Public Key Infrastructure (PKI), FG, and other technical interoperability services key necessary for interoperability and security in NG9-1-1 in North America and beyond. These services are required under standards promulgated by NENA: The 9-1-1 Association and the Internet Engineering Task Force IETF. NIOC sets the rules and policy for operating these services and performs oversight for their day-to-day operation, including compliance and finances. More information at https://ng911ioc.org.

About NENA

As The Voice of 9-1-1™, NENA is on the forefront of all emergency communications issues. The association serves its members and the greater public safety community as the only professional organization solely focused on 9-1-1 policy, technology, operations, and education issues. With more than 16,000 members in 50 chapters across the United States and around the globe, NENA promotes the implementation and awareness of 9-1-1, international three-digit emergency communications systems and NG9-1-1.

NENA also functions as the open standards development organization for emergency calling, and oversees the development of NG9-1-1 standards, including the i3 Standard for Next-Generation 9-1-1 and related standards, referred to as the "i3 family". These standards require that a small number of functional elements be operated by a central party for interoperability between jurisdictions; one of these elements is the FG for which proposals are solicited in this RFP. More information at https://nena.org.

[1] https://tools.ietf.org/html/rfc2119

Next Generation 9-1-1 Background

The traditional analog voice-centric 9-1-1 system was not designed to support many of the common communications methods and technologies in use today, such as real-time text, streaming video (including video relay services for American Sign Language users), Session Initiation Protocol (SIP), or Common Alerting Protocol (CAP), nor is it capable of conveying so-called Additional Data (for example, data associated with telematics, Internet-of-Things, smartphone applications (Apps)). There is also an increased need for responders to access additional data such as building floor plans or medical information. In addition, the need for interoperable communications within states, between states, and across international boundaries requires that we create a more flexible 9-1-1 system design with much greater data handling capabilities.

To deal with these growing needs within the emergency communications systems, NENA has developed a Next Generation 9-1-1 (NG9-1-1) emergency calling system design that includes a secure, robust, redundant, and physically diverse Emergency Services IP Network (ESInet). NENA defines the ESInet as:

> *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 inter-network (network of networks). ESInets are connected to and accept calls and data from the global internet. The term ESInet designates the network, not the services that ride on the network. See NG9-1-1 Core Services.*[2]

All NG9-1-1 emergency calls will transit one or more ESInets. The entire 9-1-1 system is transitioning to Internet Protocol (IP). IP-enabled emergency call centers ("Public Safety Answering Points" or PSAPs) will be connected to an ESInet as will all origination networks: wireline and wireless carriers, VoIP service providers, SMS/IM and other text service providers, two way interactive video service providers, including potentially those that operate entirely over-the-top. 9-1-1 Authorities may operate the ESInet and the NG9-1-1 Core Services (which include call routing, firewalls, a variety of web services, etc.) themselves, or may contract with one or more 9-1-1 Service Providers. All these entities need to be able to securely communicate over the ESInet.

ESInets are being implemented in a variety of phases and managed at different levels throughout the country. We are currently in a period of transition, during which ESInets may or may not exist at various levels (e.g., state, county, regional, local), some PSAPs will be NG9-1-1 enabled and some not, etc.

[2] https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-ADM-000.23-2020_FINAL_2.pdf

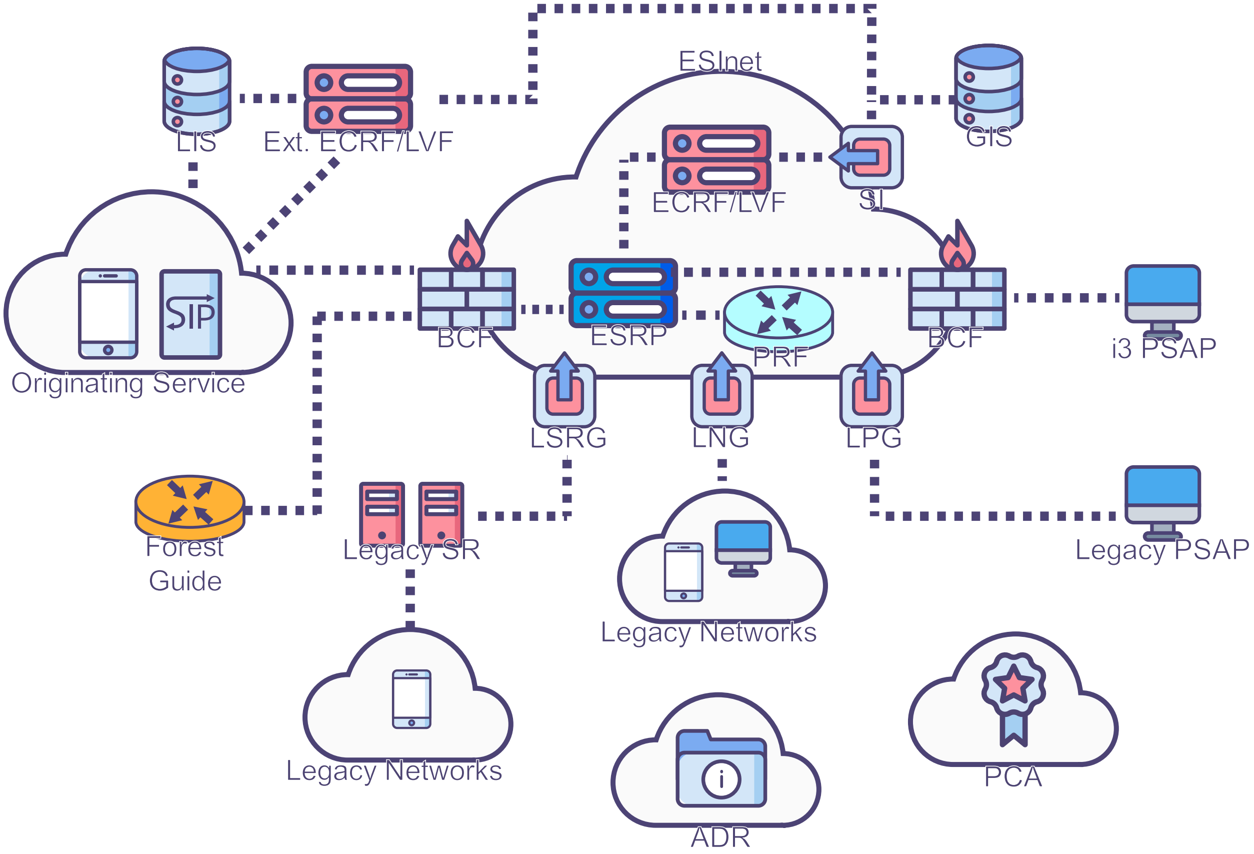


Figure 1: Simplified ESInet Diagram

The expected post-transition environment within the U.S. is that there will be a state-level ESInet in every state and territory. Within these state-level ESInets, there will likely be county, regional, or multi-county ESInets. In some cases, there might be local ESInets operated cooperatively by multiple regional authorities that are connected to multiple state ESInets and to which PSAPs in multiple states are connected (e.g., the Washington, D.C. metropolitan area could conceivably operate an ESInet connected to state ESInets operated by Virginia, Maryland, and the D.C. authorities to which PSAPs in multiple municipalities are connected; or the Wilmington-Philadelphia region might have an ESInet connected to the Delaware and Pennsylvania ESInets and to which PSAPs located in any of the three are connected). There may be multi-county regional ESInets (e.g., a Southern Illinois multi-county NG9-1-1 consortium). It is expected that neighboring ESInets will peer with each other, as well as be connected to ESInets "above" or "below" them.

Some 9-1-1 Service Providers operate at a multi-state or national level and will have to interact with many ESInets. Originating Service Providers (OSPs) likely will need to deliver 9-1-1 calls to multiple ESInets, depending on the location of the originating device. Public Safety Answering Points (PSAPs) and responders such as police, fire, EMT, hospital emergency departments or trauma centers, emergency management emergency operations centers, and the federal Homeland Security agencies need to share data received with 9-1-1 calls (such as telematics data, medical data, location data), obtained by PSAP call takers during a call, and by responders.

NG9-1-1 is built on a set of standards. The ESInet provides the environment in which NG9-1-1 Core Services (NGCS) are provided, and is the interconnect point for external networks (e.g., Originating Service Providers, downstream providers such as hospitals, etc.) and emergency services (e.g., PSAPs, responders).

The underlying standards for signaling and routing emergency calls, conveying caller location and other data, performing routing or other queries, access policies, etc., are created by the IETF. NENA standards are built on the IETF standards and specify precisely how calls are accepted, routed, and maintained, as well as how other emergency services protocols, both real-time (during call processing) and non-real-time (not during call processing) operate.

Security in NG9-1-1

The incumbent SHALL explain how it will conform to the security requirements in this section.

Credentials and Certificates

Security within NG9-1-1 and emergency services encompasses a set of mechanisms providing protection against various risks and mitigating various threats. The security mechanisms also provide for agent authentication and role-based authorization to perform actions.

These mechanisms include transport encryption of signaling and media (which provides assurance that the endpoints are who they assert, and protection against eavesdropping and alteration). These security mechanisms require a Public Key Infrastructure (PKI) that distributes appropriate X.509 certificates to agencies and agents, allows a certificate chain to be verified, provides for certificate revocation, etc.

The root of trust of the emergency services PKI is a PSAP Credentialing Agency (PCA). Agencies, service providers, and agents are issued credentials, and the public key of the credential is signed by a Certificate Authority whose own certificate is traceable to the National PCA.

These credentials are used:

- To create secure sessions between elements within the ESInet using Transport Layer Security (TLS). Nearly every communication within the ESInet is protected by TLS.
- As part of negotiation of secure keys to secure media via the Secure Real Time Protocol (SRTP).

The long-term vision is that states, service providers or the appropriate entity establish Intermediate Certificate Authorities (ICAs). States establish State PCAs or with certificates signed by the National PCA. A hierarchy of CAs can thus be created from the root PCA throughout the National PCA, such as to State and Regional PCAs. The ICA State PCA signs the certificates of each entity within its scope, such as a State ICA signing each PSAP certificate and 9-1-1 Authority certificate within the state. Regional or local PCAs would be established to issue certificates to agents within the agencies whose certificate is signed by the State PCAs. Through this framework the hierarchy of the PKI for ESInets would be complete.

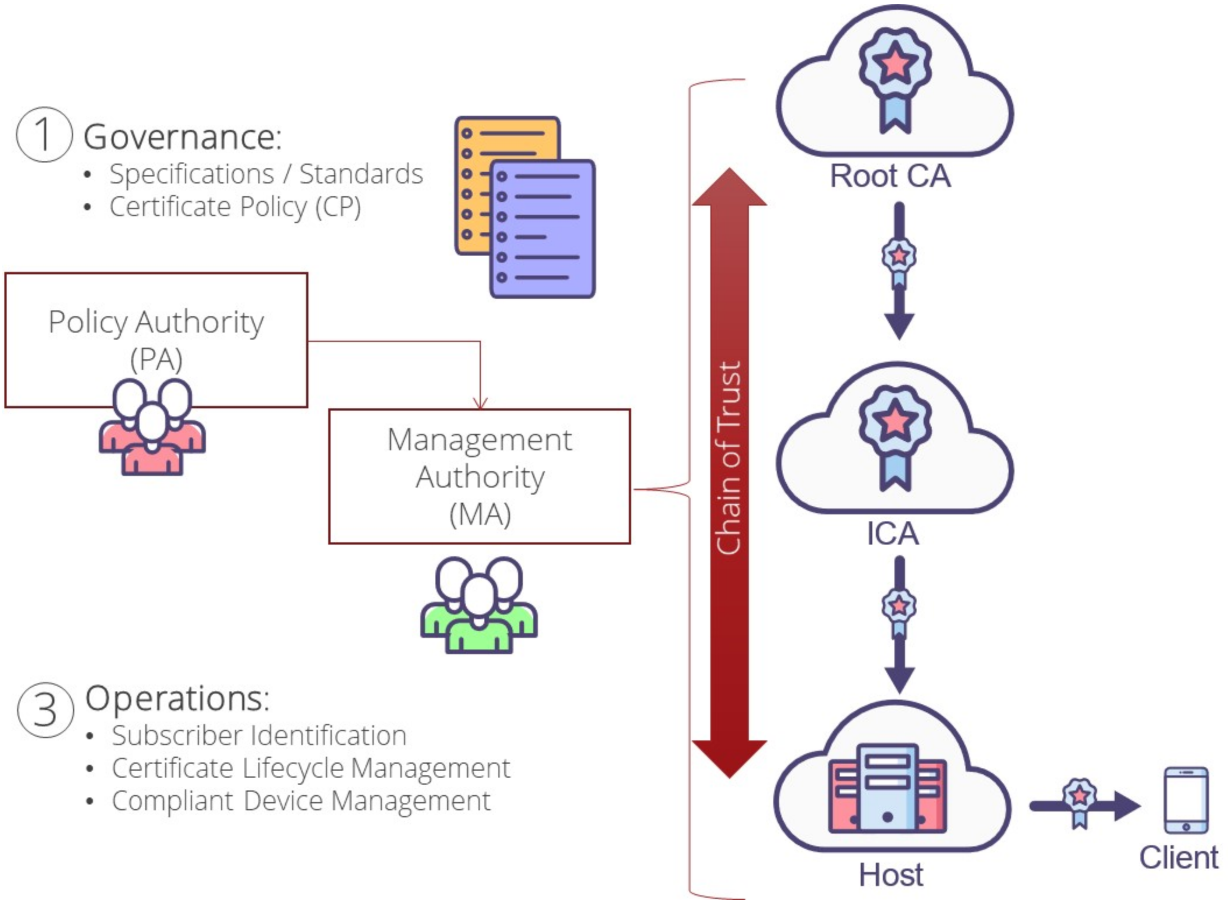

1 Governance:
• Specifications / Standards
• Certificate Policy (CP)
Policy Authority (PA)
Management Authority (MA)
3 Operations:
• Subscriber Identification
• Certificate Lifecycle Management
• Compliant Device Management
Chain of Trust
Root CA
ICA
Host
Client

Figure 2: NG9-1-1 Public Key Infrastructure

In addition to the use of the PKI and Public Key cryptography, the following security assumptions apply to the NENA ESInet as well as to the FG and should be considered by the RFP respondents:

- All physical locations containing FG, Core Services, or ESInet system functions or applications SHALL be physically secure with controlled personnel access procedures, including the recognition that some personnel will require a higher level of access authorization than other personnel.
- FGs SHALL be protected with appropriate access control mechanisms such as firewalls. Session Border Controllers (SBC) and firewalls SHALL be deployed at all ESInet host sites between other ESInets, 9-1-1 Service Providers, and telecommunications service providers including Internet Service Providers (ISP).
- Firewalls SHALL be deployed between the PSAPs and the ESInet permitting the use of Access Control Lists (ACL) to provide specific host-to-host traffic only
- All addressable resources with the ESInet SHALL have separate addresses for each ISP used by the ESInet, in order to prevent an attack on, or failure of one ISP, from negatively impacting the entire ESInet.
- Internet access at the PSAP level will be managed by the use of ACL managed at the regional or state-level 9-1-1 Authority.
- ESInets will use Border Gateway Protocol (BGP) to interconnect with other ESInets.
- ESInet service, application or other vendor, and PSAP personnel, who need access to an ESInet or services that run on it, or to applications utilizing the ESInet, SHALL use the specified Single-Sign-

On (SSO) mechanism for authentication of all individuals. The single-sign-on mechanism will include the level of system access authorized for each individual and their particular job role or assignment. The SSO mechanism enables use of the credentials assigned to agents.

- Data access to data owned by an agency is limited by the rights specified by the data owner using a standardized Data Rights Management (DRM) mechanism. Data owners create XACML based rules as described in the NENA i3 standard and all access to such data is governed by these rules.
- Normal Internet security best practices are expected to be followed. For example, DNS security is used to verify the authenticity of data retrieved from the DNS. Coverage regions maintained or accessed by the FG are digitally signed using credentials traceable to the PCA.

LoST Security

Coverage region information is digitally signed by the authority creating it (as described in RFCs 5582 and 6739) and remains signed as it is transported in query responses and synchronizations. Coverage regions that are supersets of underlying mappings or coverage regions are signed by the entity creating them. For example, a leaf node may be provisioned with a mapping or have a mapping injected into it that maps service URIs for a specific PSAP within the leaf node's area of authority (an area of a city, say). The local emergency services authorities signed the mapping with their credentials. The leaf node may inject a coverage region encompassing its area of authority with its AUS into an intermediate parent node (a county LoST server, say). That coverage region is signed with the credentials of the authorities responsible for the leaf node. The intermediate parent node (the county LoST server in this example) may inject a coverage region encompassing its area of authority (the county) into a parent node (perhaps a state LoST server), which may inject its area of authority into a FG. Each LoST server and client can verify that a mapping or coverage region is signed with credentials traceable to the PCA. However, it may be difficult for an entity to verify that a mapping or coverage region was signed by the *correct* authorities, as opposed to some other entity holding PCA-traceable credentials but not authoritative for the region in question.

LoST has a chain of trust in addition to signed data. The FG only accepts coverage regions from verified sources, for example, the FG will only accept a coverage region for a state from appropriate authorities for that state. The state LoST server will likewise only accept coverage regions from appropriate authorities for the region (e.g., a county), and so forth. By this chain, a client can trust that it is receiving accurate information.

Single Sign-On

All NG9-1-1 agents (staff authorized to perform various tasks) use Single Sign-On (SSO), as described in i3v3,[3] to authenticate and authorize operations. SSO allows agents to perform tasks per their authorization, and to use certificates traceable to the PCA. Elements and functions use SSO to identify agents and authorize their actions.

[3] Public review draft available at: https://dev.nena.org/higherlogic/ws/public/document?document_id=16133&wg_id=eca27a3d-a4c7-4d67-bb06-b3bb241df44e. Most current version available upon request to rfp@ng911ioc.org.

NG9-1-1 Protocols

As described and specified in i3v3, a number of protocols are used as part of NG9-1-1. These include communication protocols carrying data such as location and incident data and establishing and conveying interactive media streams between calling devices and call takers, most notably SIP, the LoST protocol to determine the routing for a call or validate a civic location or to lookup the authoritative ECRF or LoST server for a region, LoST-Sync (RFC 6739) to maintain synchronized mappings between ECRFs/LoST servers, and HTTPS to access a wide variety of information, among others. Since NG9-1-1 uses IETF protocols, and an ESInet is a network using Internet Protocol (IP), a number of lower-level protocols and functions are necessarily used, such as the Domain Name Service (DNS) to map domain names to IP addresses, various routing protocols to correctly route IP packets, etc. Transport Layer Security (TLS) is used as a component of many protocols to provide protection against eavesdropping or alteration of protocol exchanges, and mutual authentication via public-key certificates.

Governance and Oversight

Incumbents SHALL describe how they anticipate functioning under the governance model below. Additionally, incumbents SHALL certify that the proposed solution is free of conflicts of interest with the governing body.

Proposers understand that the FG will be subject to NIOC, which is a governing body independent from the NENA office. The NENA office will provide staff that administers the contract with the proposer to operate the FG, however, all policies, procedures, budget and fee schedule will be established by NIOC. NIOC will ensure that the program is run ethically, and with full transparency, including with books open to the public.

NIOC is composed of a variety of seats representing public safety interests within the PKI and seats include:

- The NENA chief executive officer ("CEO") (non-voting)
- The president of the Board
- One member from the NENA Development Steering Council
- One member from the NENA 9-1-1 Core Services Committee
- One member representing a U.S. state, provincial, or national non-U.S. authority with responsibility for operating an NG9-1-1 network
- One member representing local or regional 9-1-1 authorities with responsibility for operating an NG9-1-1 network within a region smaller than a US state or province, such as a county, metropolitan area or a council of governments
- One member representing commercial providers of NG9-1-1 core services ("Core Services Member")
- One member representing commercial providers of NG9-1-1 end-user products
- One member representing organizations with a direct responsibility for handling 9-1-1 emergency calls
- One member representing elected officials who does not represent a public safety agency, with oversight of 9-1-1 services
- One member representing public safety associations not otherwise represented

Additionally, NIOC includes several non-voting seats, such as on behalf of the NENA staff that administers the contracts entered into with NIOC approval as well as the US Federal Communications Commission and its Canadian counterpart, CRTC.

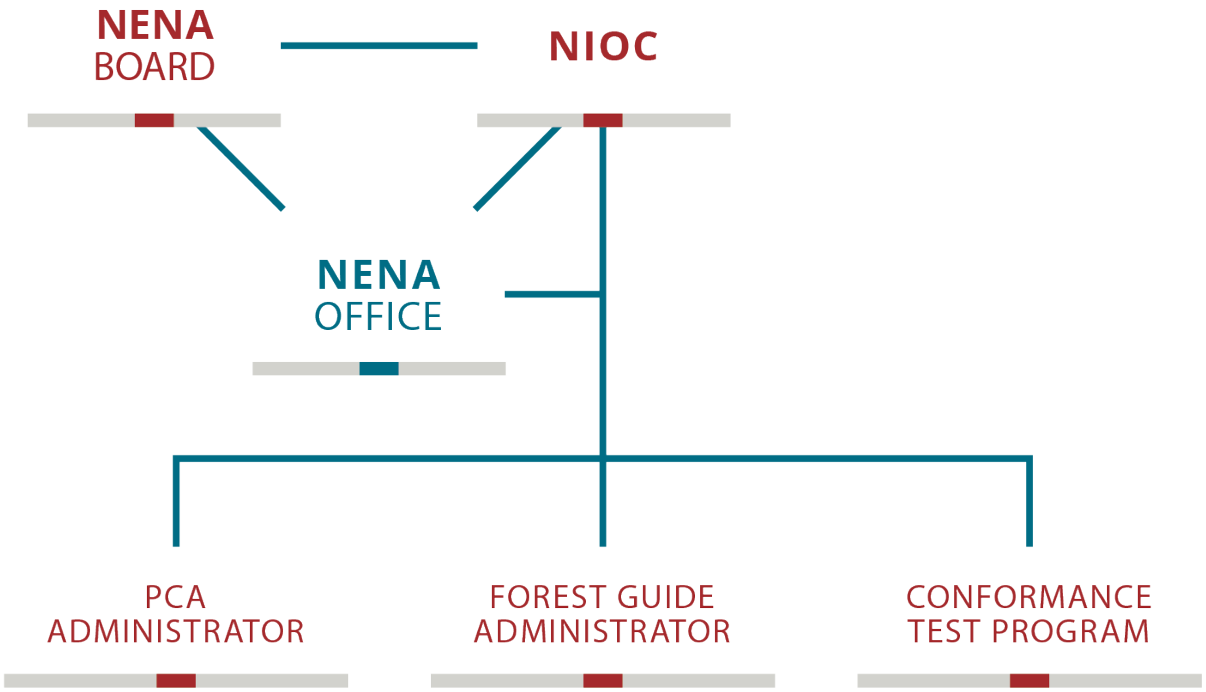


Figure 3: Governance Model

Proposers are advised that any selection or offer by the NENA office is contingent on approval by NIOC, and that the proposer will be contractually obligated to operate under its policies.

LoST, Trees, and Forest Guides

Following is a description of how a FG functions. Proposers SHALL describe how their proposed solution conforms to the normative requirements of the cited technical standards and asserted expectations in this section.

LoST (RFC 5222) servers map locations and services or servers. LoST servers maintain sets of service information for geographic regions. In an abstract sense, LoST is somewhat analogous to DNS and packet routing. All rely on concepts of authoritative sources and a delegation hierarchy to distribute the work of maintaining accurate and up-to-date information. DNS uses a hierarchy of labels or zones (a root zone maintains knowledge of authoritative servers for each top-level domain (TLD) such as “com”, and each top-level authoritative server maintains knowledge of authoritative servers for second-level domains within each TLD (such as “example.org”); that is, the root zone delegates authority for each TLD to an authoritative server for that zone, which in turn delegates authority for each second-level zone to an authoritative server for that zone, which in turn might directly serve or further delegate authority for sub-domains to authoritative servers for those domains). Resolving a query (such as determining an IP address of a host) could require starting at the root and determining an authoritative DNS server for the TLD of the host, then querying that server for an authoritative DNS server for the secondary domain of the host, and so forth, until reaching a DNS server that is authoritative for the lowest level of the host’s name. However, caching allows many steps to be skipped. Signed DNS records allow results to be relied on (especially when accessed from non-authoritative servers). IP packet routing uses IP addresses rather than domain name labels, but similarly relies on the concept of authoritative information for a range of addresses (denoted by prefixes); an entity that controls a block of IP addresses designates one or more autonomous systems (AS) that are able to route packets to or from that address range (prefix);

autonomous systems advertise the prefixes they handle to their peers, which maintain tables so that they can forward packets to the appropriate AS. Routers further away aggregate prefixes in their tables to simplify routing decisions and optimize lookups.

LoST delegates information by geographic region, using service boundaries. Countries can be thought of as analogous to TLDs (coincidentally, in the DNS, each country is assigned a two-letter TLD and has authority for it), with states or territories being conceptually somewhat like secondary domains. LoST servers maintain coverage regions and/or mappings. Coverage regions identify an authoritative LoST server for a specific region (as an Application Unique String (AUS) in the form of a domain name), while mappings identify service URIs to access a specific service for a location. LoST servers are hierarchically organized into "trees." A tree is a set of LoST servers ranging from a root node to leaf nodes that maintain information for one service for one civic or geospatial coverage region. Trees are hierarchical sets of servers; the root of a tree has knowledge of the entire coverage region of the tree. Typically, the root's knowledge is a set of smaller regions that together constitute its region, and for each it knows the AUS, in the form of a domain name, to use to contact the child LoST server that is authoritative for the region. In some cases, instead of the AUS for a child server, the root knows the actual service URIs for the region. A set of trees for one service is called a forest. The concept of root, intermediate, and leaf servers is conceptual; a region could potentially have only one single LoST server that is the root and maintains all service URIs, without intermediate child servers, or each level of a tree might have service URIs for some sub-regions, and AUSs for other sub-regions. Each server is typically a cluster of servers that are reachable via the same URI and that share identical data, for redundancy, load-balancing, etc.

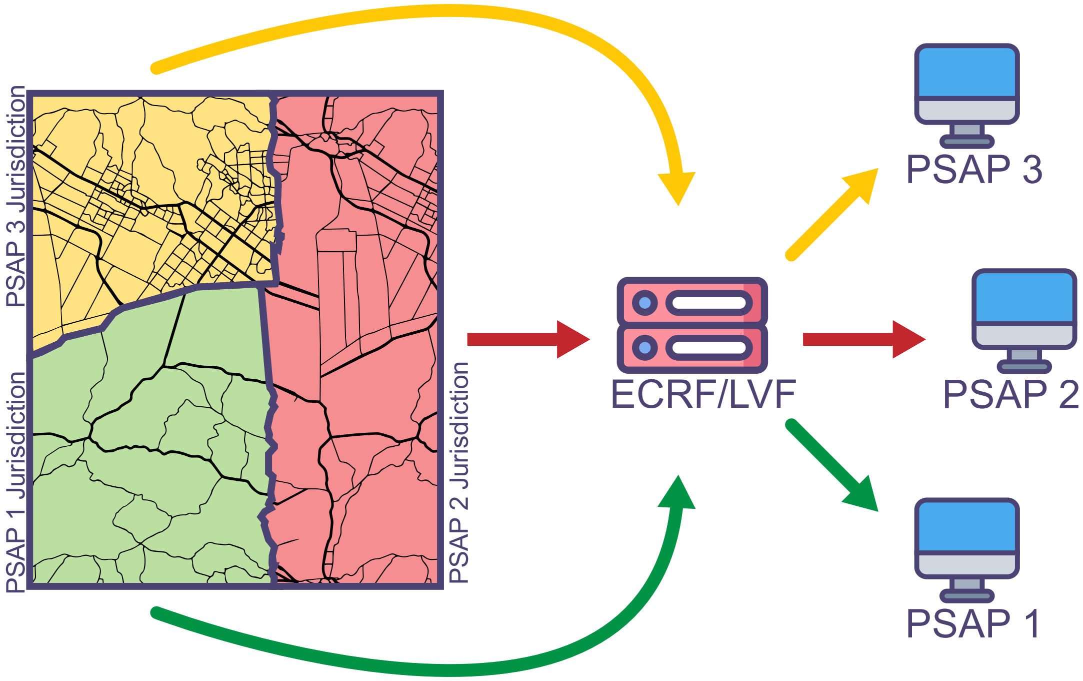


Figure 4: LoST Server Boundaries and Geospatial routing

The LoST RFCs define civic and geospatial location formats (profiles) as being in separate trees (even if the regions are identical, e.g., a civic region specifying a state and a geospatial region as a set of polygons encompassing the state). i3 specifies that LoST servers performing an Emergency Call Routing Function (ECRF) and a Location Validation Function (LVF) are in separate trees. Trees that cover the same region but differ in the service URNs mapped, or in civic versus geospatial profiles, are conceptually different trees, but this has little practical difference, as the same LoST servers are expected to serve them. Trees that cover different regions can be served by the same LoST servers as well, but this is not expected to be common in most cases. Trees that support ECRF versus LVF do need to be separable, that is, it needs to be possible to deploy different sets of LoST servers for ECRF and LVF services.

For emergency services, urn:service:sos and urn:service:test.sos (and their subservices such as urn:service:sos.police) and services within urn:emergency:service (e.g., urn:emergency:service:sos, urn:emergency:service:responder) are the service URNs. Note that urn:emergency is for internal (within an ESInet) use only; it is not visible outside an ESInet. The urn:service:sos and urn:service:test.sos (and their subservices) are visible universally.

The LoST servers within a tree may be operated independently from each other or not (and could be co-located with each other), and a LoST server could be part of more than one tree (if it maintains information for more than one service and/or geographic area).

An FG is a LoST server that maintains information on all trees in a forest (e.g., a national or country FG has coverage regions for each tree root for one service in one country). Multiple FG servers could be co-located (i.e., one server cluster could operate as the FG for multiple services in a country, or one service for multiple countries, or both), e.g., Sweden, Norway, and Denmark could decide to jointly operate a Scandinavian FG, or could have one FG for each country co-located in a single server cluster. FGs can peer with each other, and thus maintain coverage information for other forests. This is expected to be common with neighboring countries or regions.

This request for proposals is for a FG to serve at least the United States; accordingly, it will interchangeably use the terms “North American Forest Guide” or “U.S. Forest Guide” (and/or the acronym “FG”). However, responders are encouraged to describe how their approach is scalable to cover regions outside of the United States or North America, subject to oversight by NIOC.

NG9-1-1 defines two roles for LoST servers: an Emergency Call Routing Function (ECRF) and a Location Validation Function (LVF). The ECRF service is the exemplar use case for LoST, as it allows emergency calls to be routing to the appropriate PSAP for the call’s location. The ECRF service is used in real time as calls are routed. As calls progress, different ECRFs may be queried, and may return different information. For example, an ECRF outside an ESInet typically returns a service URI that is an entry point into an ESInet (i.e., a URI that resolves to an Emergency Services Routing Proxy (ESRP) or Border Control Function (BCF) at the gateway into an ESInet), while an ECRF inside an ESInet may return a service URI for a PSAP or another internal ESRP. The LVF service is used in advance of call origination, typically during provisioning of a Location Information Server (LIS) or other facility that maintains civic address information, or to validate a civic address entered by a customer of an over-the-top (OTT) service provider. i3 specifies that these two functions are considered their own trees, so that they can be deployed using physically separate LoST server clusters if desired (e.g., to permit different allocations of capacity, bandwidth, attack mitigation, or other resources).

The same LoST server may exist within multiple trees. For example, an ECRF may authoritatively answer queries for both civic and geospatial profiles for both “URN:SERVICE:SOS” and “URN:SERVICE:TEST.SOS” for one region. It is not necessary to be able to identify in advance of a query which of these trees a specific ECRF serves, as the ECRF either will or will not be able to answer a query for a particular profile for a particular service for a particular location. The same applies for the LVF function. However, NENA i3 requires that the ECRF and LVF services be separable, that is, an organization operating a LoST server cluster may choose to make the ECRF and LVF server clusters physically separate. An organization might do this in order to provide higher levels of service for an ECRF while shielding it from the potentially bursty network traffic load of an LVF. (Other organizations might choose to use the same sets of servers for both, able to offer the high service level demanded of an ECRF.) In order to permit this separability, any entity querying a LoST server needs to be able to resolve an AUS into a URI for a specific server that offers the required service (EVRF or LVF).

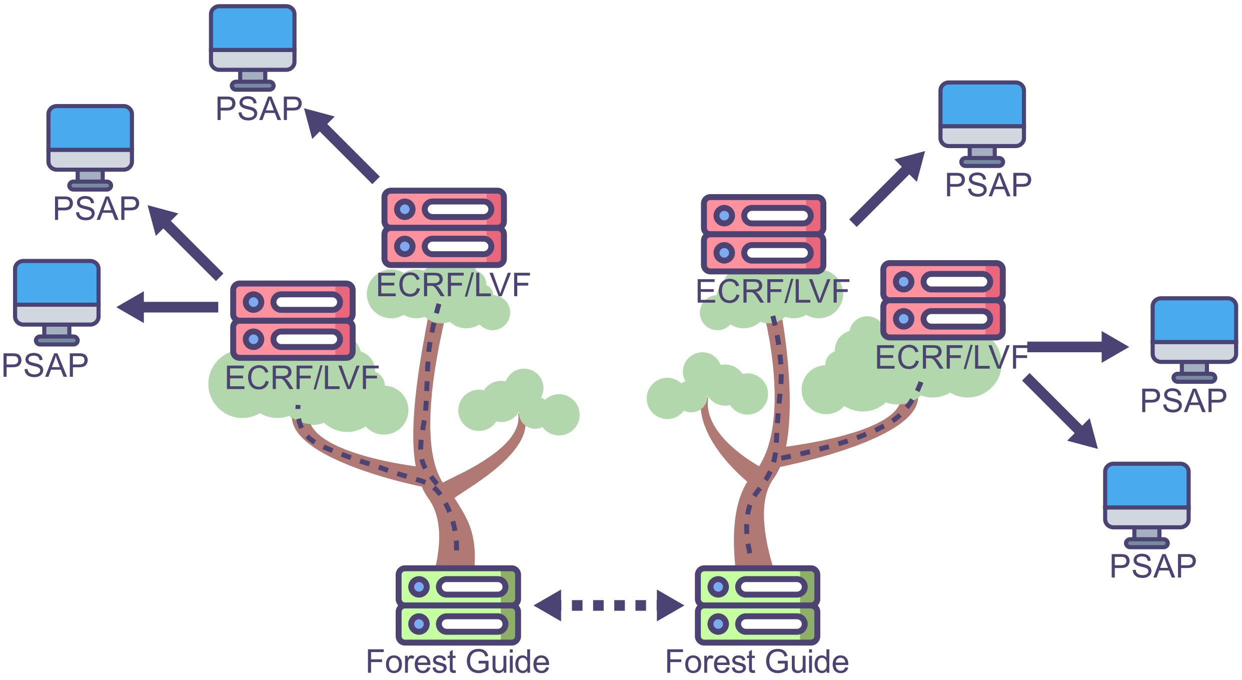


Figure 5: LoST (ECRF/LVF) Tree

For example, consider a PSAP that serves, say, a portion of the town of Springfield in the fictional U.S. state of Progressus. The town of Springfield might operate a LoST server that is authoritative for the town for both ECRF and LVF services. For ECRF purposes, this LoST server maintains service mappings for all PSAPs that serve the town for all defined services for both civic and geospatial profiles. Each of these mappings contains either civic or geospatial regional coverage boundaries and a SIP service URI. For LVF purposes, there is a set of layers allowing each unique street address to be verified. Conceptually, there is one such mapping per service per civic/geospatial per ECRF/LVF. In practice, the data can be internally organized in any desired way (e.g., each coverage region as a set of geospatial zones and/or a set of civic boundaries, and URIs for all services).

A client can ask a LoST server for service URIs to access a desired service that serves a specific location. For our purposes, the most important service is "urn:service:sos". The location can be expressed as either civic or geospatial. Civic (also called postal) addresses can include varying levels of specificity (e.g., country, state, county, city, street, street address, unit). Geospatial locations may be a point or a shape. A shape may represent an area of uncertainty within which the desired point is located within a certain probability (e.g., the desired point might be within a circle with an area of 500 meters with an 80% confidence level). LoST also uses shapes (as well as civic locations) to represent service areas (e.g., PSAP x has a service area defined by a set of boundaries that form a polygon).

A client can also ask a LoST server for the list of services available for a location.

Normally, origination devices that handle their own emergency call routing query a caching LoST resolver rather than the authoritative LoST server, although they may do so. Such origination devices obtain their emergency call routing URI when their location changes significantly, or if they move outside a previously obtained service boundary, and thus can normally initiate an emergency call without needing to query a LoST server. Origination networks that handle location and routing of emergency calls may maintain their own LoST server or an equivalent function, or they may query an authoritative LoST server. Normally, only authoritative LoST servers query a FG. Authoritative LoST servers normally permit queries by any entity, but under stress may restrict queries to a set of authenticated clients. Parent nodes (intermediate or tree root) may likewise restrict queries when under stress, such as only permitting queries from child LoST servers authorized to inject coverage regions, which allows recursive LoST queries to propagate from tree leaf to root as needed. Similarly, FGs may restrict queries to only tree roots or equivalent nodes when under attack or subject to unusual stress.

LoST servers are contacted by resolving an AUS, which has the form of a domain name (e.g., "lost.example.net"), using U-NAPTR as described in RFC 5222 and RFC 4848. RFC 5222 defined the NAPTR service tag "LoST". A work-in-progress proposes to add the "LoST-Validation" service tag. Without the "Lost-Validation" service tag, it is not possible to resolve an AUS into a LoST server for LFV versus ECRF services. Assuming the "LoST-Validation" tag is defined, an entity uses U-NAPTR to resolve an AUS into a URI for a server that was identified using either the "LoST" or "LoST-Validation" service tags.

State-level (or the largest area within a state level) ECRF and LVF tree roots provision their coverage regions and AUS into the national FG. The CONTRACTOR of the national FG will provision NAPTR records so that other national FGs and authorized entities can contact the FG by starting with a well-known AUS in order to use LoST-Sync to exchange their coverage regions or mappings (that is, peer).

Entities within an ESInet that perform a LoST query always request recursion. LoST servers within an ESInet must support recursion. This allows LoST queries to function even during an event that causes one or more LoST servers (potentially including the FG) to reject queries from non-authorized entities (e.g., only answering queries from tree roots that have injected their coverage regions into the FG, or other authorized entities). For example, a PSAP in, say, Oregon, needing to transfer a call to an agency in a different state, say California, may query its local ECRF using the California location, requesting recursion; the local ECRF will query its root ECRF, requesting recursion; the Oregon root ECRF will query the internal national FG; the internal national FG doesn't support recursion, so will return a refer with the AUS for the root ECRF of the region containing the location, in the example, California's root ECRF. The Oregon root ECRF will then need to query the California root ECRF. This requires that the Oregon root ECRF have connectivity to reach the California ECRF, and that the California root ECRF will answer a query from the Oregon ECRF, even if under stress. NENA STA-010.3 permits internal ECRFs to refuse queries from entities they do not "know" (which could be interpreted as other nodes within their tree). If the internal national FG returns an AUS for the internal root ECRF, then Oregon's root ECRF may not have connectivity to reach the California root ECRF. Requiring the internal national FG to support recursion would resolve this but would impose additional load on the national FG. Further, whatever answer the California root ECRF returns needs to be reachable by the Oregon PSAP. It might be desired that the California root ECRF would return a mapping containing a URI for a border ESRP, but that requires that the California root ECRF be aware that the query is from an out of state entity. One approach to this would be to take advantage of DNS by providing different NAPTR records depending on the querier (queries for a California ECRF AUS resolve to a URL for the internal or external California root ECRF depending on if the query is done inside or outside the California state ESInet). Proposers are encouraged to describe how their approach will handle this case. TODO: resolve this paragraph. Likely will need clarifying text in NENA STA-010.3 and possibly discussion within i3.

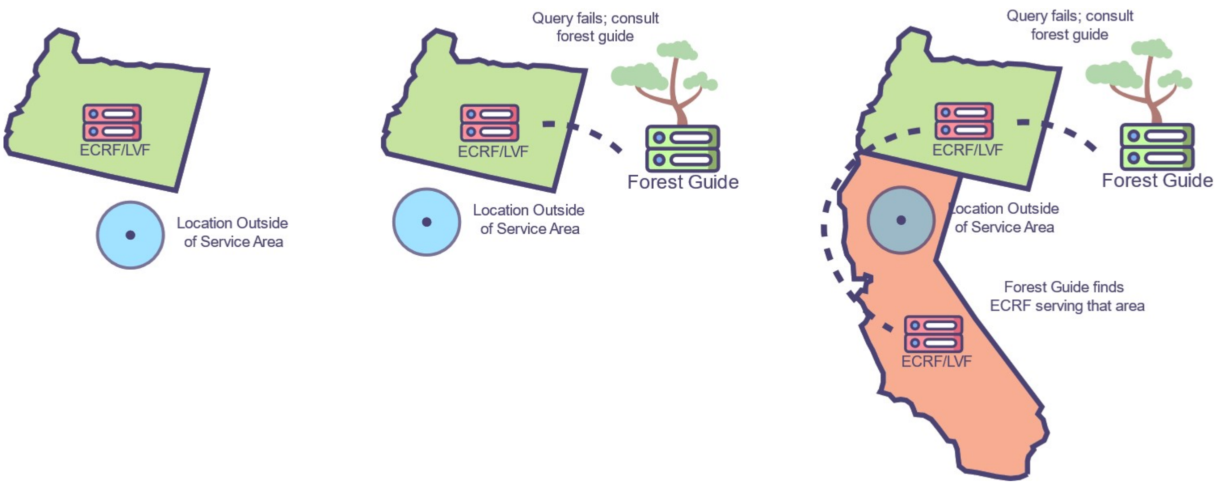

ECRF/LVF
Location Outside of Service Area
Query fails; consult forest guide
ECRF/LVF
Forest Guide
Location Outside of Service Area
Query fails; consult forest guide
ECRF/LVF
Forest Guide
Location Outside of Service Area
Forest Guide finds ECRF serving that area
ECRF/LVF

Figure 6: Recursive query where ECRF consults Forest Guide

Because ECRF is a critical service, LoST servers in an ECRF tree, including the FG, should verify that NAPTR records containing the "LoST" service tag exist and are usable for each AUS with which they are provisioned. That is, after a coverage region is added or updated, the server should perform U-NAPTR resolution on the AUS to verify that a URI is obtained. The server does not need to use the URI to contact the server and verify that it is able to resolve queries or redirect. Assuming the "LoST-Validation" service tag is defined, LoST servers in an LVF tree, including the FG, should perform the same sanity check using the "LoST-Validation" service tag. This is a basic sanity-check step; it does not verify that a server is reachable and returns correct information, only that plausible information is loaded into the DNS at the time if the check.

Statement of Work/Need

Requirements

Multiple Forest Guides

For emergency services, urn:service:sos and urn:service:test.sos (and their subservices) and services within urn:emergency:service (such as urn:emergency:service:sos or urn:emergency:service:responder) are the service URNs. Note that urn:emergency is for internal (within an ESInet) use only; it is not visible outside an ESInet. The urn:service:sos and urn:service:test.sos services are visible universally. NG9-1-1 needs a publicly available FG (along with publicly available LoST server trees providing ECRF and LVF services). This requires that there be FGs for internal and external use, with identical urn:service:sos (and urn:service:test.sos) data in both, and urn:emergency data only accessible via the internal one. The CONTRACTOR may choose the deployment options to satisfy this (e.g., the internal FGs could propagate urn:service:sos (and urn:service:test.sos) data to the external ones, or vice-versa, or all services could exist in all FGs with the external FGs never returning urn:emergency results, although the last option carries greater risk of leaking internal data). The internal FGs MUST be accessible by any LoST server within any ESInet. During the transition period when there might not be an intermeshed network of state ESInets nor a national ESInet, this may require special operational considerations (e.g., VPN connections between the network hosting the internal FGs and multiple state or regional ESInets, replicated internal FGs within various ESInets, or other arrangements).

i3 requires that the ECRF and LVF services be separable, so that each state-level or other region can decide to provide ECRF and LFV services using consolidated or separate server clusters. The rationale is that ECRFs are used in real-time during call routing, while LVFs are used in advance, when data is provisioned. This separability (for all service URNs) needs to be maintained throughout the tree structure, from FG to leaf node.

There are thus separate trees and forests for internal and external LVFs for urn:service:sos, and ECRFs for all services.

The LoST RFCs define civic and geospatial location formats (or profiles) as being in separate trees. Currently, there are twenty forests for emergency services within the U.S.:

- internal, urn:service:sos, ECRF, civic;
- internal, urn:service:sos, ECRF, geospatial;
- internal, urn:emergency:service:sos, ECRF, civic;
- internal, urn:emergency:service:sos, ECRF, geospatial;
- internal, urn:emergency:service:test, ECRF, civic;
- internal, urn:emergency:service:test, ECRF, geospatial;
- internal, urn:emergency:service:responder, ECRF, civic;
- internal, urn:emergency:service:responder, ECRF, geospatial;
- internal, urn:emergency:service:agencyLocator, ECRF, civic;
- internal, urn:emergency:service:agencyLocator, ECRF, geospatial;
- internal, urn:service:test.sos, ECRF, civic;
- internal, urn:service:test.sos, ECRF, geospatial;
- external, urn:service:sos, ECRF, civic;
- external, urn:service:sos, ECRF, geospatial;
- external, urn:service:test.sos, ECRF, civic;
- external, urn:service:test.sos, ECRF, geospatial;
- internal, urn:service:sos, LVF, civic;
- internal, urn:service:sos, LVF, geospatial;
- external, urn:service:sos, LVF, civic;
- external, urn:service:sos, LVF, geospatial

The Internet Assigned Numbers Authority (IANA) maintains the URN namespace registries in which urn:service:sos, urn:service:test.sos, and urn:emergency:service are registered.

While no additional service URNs are currently expected or contemplated, new services could be added to any registry at any time. If and when new services are added that could reasonably be used in an ECRF or LVF LoST query, the CONTRACTOR is expected to support them within a reasonable time after they are added (e.g., 120 days). The CONTRACTOR may ask NIOC for advice as to which new services could reasonably be used in an ECRF or LVF LoST query. NIOC MAY direct the CONTRACTOR to the NENA Development Group (NDG) and/or the expert listed for the appropriate registry. Time waiting for a response to such a query will not be counted against the reasonable time to support requirement. The proposer SHALL explain its expectations in implementing additional service URNs.

The FG needs to differentiate if it was accessed for an ECRF or LVF forest so that it can return an AUS for the corresponding authoritative LoST server. This differentiation may be accomplished in various ways, such as a multihomed server using the IP address of access, or, since LoST uses HTTPS for transport, using the Server Name Indication (SNI) to distinguish among the logical FGs it is acting as. The proposer SHALL explain how it will handle such queries.

Note that discovery mechanisms for the different trees and FGs are not currently well-defined (i.e., currently it is not specified how a client determines which resolver serves the appropriate tree, nor how a LoST server in one tree determines which FG to contact, or how provisioned data such as AUSs can be validated to ensure tree coherence, etc.), however, for ECRF versus LVF purposes, different U-NAPTR service tags are expected to be used (the "LoST" service tag for ECRF and the "LoST-Validation" tag for LVF). Proposers SHALL describe what discovery method they propose, and how/whether this method conforms to a consensus standard. If the method does not, the proposal SHALL describe how the method SHALL be incorporated into a consensus standard, preferably under NENA or IETF as appropriate.

Three-Dimensional LoST Queries

It is envisioned that the LoST MAY be updated in the future to support three-dimensional geospatial queries. This has significant impacts to provisioning and managing of an FG. In their responses, proposers SHOULD describe how their solution may or may not support three-dimensional LoST queries and what future impacts 3D LoST queries may have on managing of an FG. For example, three-dimensional queries may require additional trees.

LoST Extensions

The FG, as with all NG9-1-1 LoST servers, is required to support the Call and Incident ID Extension to LoST, as defined in i3.

LoST Planned-Changes is primarily useful for LVF leaf nodes, and so is not expected to impact the FG; thus, support for Planned-Changes is OPTIONAL in the FG.

Proposers SHALL describe their support for these extensions.

Data Stored

During the transitional period for NG9-1-1 deployment, it's possible that not all state-level regions have a state-level ESInet, state-level LoST servers, etc., and so various sub-state level LoST servers may inject coverage regions into the FG in lieu of having a state-level do so. The FG will maintain information for states, state equivalents, and at sub-state levels in the absence of a state or state-equivalent entity.

Per NENA i3, all geodetic data for the Forest Guide SHALL use WGS84.

The FG stores information about available trees. Each tree is a hierarchy of LoST servers that are authoritative for a region and that respond to ECRF or LVF queries. Trees are hierarchical, with a root node at the base being responsible for a large (nominally, state-level) area. The root stores the coverage areas and either AUSs for child nodes to which the sub-region is delegated, or service URIs. Intermediate nodes store information encompassing an area smaller than the root (e.g., a multi-county sub-state region, a county, or a sub-county). Intermediate nodes store coverage regions for smaller areas, and like state-level root nodes, either an AUS for a child node authoritative for the area or service URIs. Leaf nodes have no child nodes, they store coverage regions with service URIs.

The FG stores the coverage region of each tree and an AUS for the tree's root LoST server. The FG called for in this document is for the United States, and as explained above, is logically a series of FGs. These FGs store state-level regions in geodetic or civic forms (using the "geodetic-2d" and "civic" profiles as defined in RFC 5222 and referenced in i3). The geodetic form is a set of one or more polygons that describes the borders of a state or state equivalent (such as territories, federal districts, possessions, etc.) while the civic form uses the format as described in i3 and RFC 5139 and identifies a state or state equivalent. State-level entries have <country> and <a1> elements (<a1> is used for states and state equivalents). Entries for regions smaller than states have additional elements (e.g., <a2> for a county, <a3> for a city). In addition to a location, each entry has an AUS that normally is that of a state-level LoST server (either for an ECRF or an LVF, and for one service, as described above).

The FG is expected to peer with any other U.S. FGs, all holding the same or roughly equivalent sets of data, for data replication and resiliency. The U.S. FG is also expected to peer with other FGs that hold non-US data, for example, a Canadian FG, potentially European, Asian, etc. FGs, so that queries for locations outside the US may be directed to an appropriate tree root or FG. The US FG may also hold coverage region information for non-US areas, such as Canadian provinces near the US border, etc., so that queries for border region locations may be directed to an appropriate LoST server.

The coverage regions stored by the FG are digitally signed by the responsible authorities, using credentials traceable to the PCA (this is discussed in RFCs 5582 and 6739).

Proposals SHALL describe how it will handle data storage and provisioning.

While LoST functions in only 2 dimensions at this time, it is expected that LoST queries MAY support 3D routing queries in the future. While 3D LoST queries may be helpful in some areas, such as routing to different PSAPs on an interstate overpass as opposed to the city street below it, it is acknowledged that such utility is an edge case for any LoST queries that may be handled by a FG. Nonetheless, Proposers SHALL describe how their solution MAY or MAY NOT be upgradeable to support 3D routing queries.

Interfaces

Supported Queries

As a LoST server, the FG supports <findService>, <getServiceBoundary>, <listServices>, and <listServicesByLocation> queries. The response to a query may depend on the credentials and identity of the client, and the FG may refuse queries from unauthenticated clients or clients that do not represent configured data when under stress. The FG is not expected to support recursion, as the primary intent of a FG is to obtain an AUS for a tree root LoST server. The response to a <findService> query is normally a <redirect> element containing the AUS for the authoritative LoST server for the requested location (e.g., the root node of the state-level LoST tree).

Provisioning Interfaces

The FG supports the Spatial Interface (SI) as defined in i3, which may be used by authorized authorities to configure their service boundaries.

The FG SHOULD NOT support any proprietary provisioning interfaces for coverage regions as well as operating parameters, etc., except as explicitly required due to gaps in standardization and in any fashion which does not affect interoperability between disparate NG9-1-1 systems. Proposers SHALL describe what proprietary interfaces, if any, their solution requires, with certification that such interfaces will not materially affect provisioning of FG data between jurisdictions.

The FG supports the LoST-Sync protocol of RFC 6739, as described in the following section. Proposers SHALL explain how their implementation supports LoST-Sync.

Updates Accepted from Authoritative LoST Servers

The FG supports the LoST-Sync protocol of RFC 6739, which provides the <getMappingsRequest>/<getMappingsResponse> and <pushMappings>/<pushMappingsResponse> exchanges. State-level tree roots use <pushMappings> to add or update their coverage regions into the FG. During the transitional period before ubiquitous NG9-1-1 deployment, sub-state regions may inject or update their coverage regions into the FG. In some cases, a new state-level authoritative LoST server may inject a new coverage region that subsumes existing coverage regions. For example, in the absence of a state-level LoST server, one or more county or other regional LoST servers may have added their coverage regions into the FG; when a state-level LoST server later exists, it will be authoritative for the state, and will inject its statewide coverage region into the FG. The FG needs to detect this and remove the now-subsumed regions in favor of the statewide one. Proposers SHALL explain the workflow for validating such changes in coverage regions.

The coverage regions stored by the FG are digitally signed by the authorities responsible for the region, using credentials traceable to the PCA (this is discussed in RFCs 5582 and 6739). The FG will use appropriate policies and procedures, as approved by the NIOC, to determine which entities are authorized to inject or update information for which areas. This verification is vital to maintaining a chain of trust as described above.

Peering and Synchronization

FGs can peer with each other, and thus maintain coverage information for other forests. This is expected to be common with neighboring countries or regions.

The FG is expected to peer with any other U.S. FGs, all holding the same or roughly equivalent sets of data, for data replication and resiliency. The U.S. FG is also expected to peer with other FGs that hold non-U.S. data, for example, a Canadian FG, potentially European, Asian, etc. FGs, so that queries for locations outside the US may be directed to an appropriate FG. The US FG may also hold coverage region information for non-US areas, such as Canadian provinces near the US border, etc., so that queries for border region locations may be directed to an appropriate LoST server.

ESInet operators MAY query an authoritative reference FG at any time, however, they SHOULD maintain a local, up-to-date replica for survivability purposes and to reduce dependence on a single service, no matter how highly available. Proposers SHALL describe how their service supports provisioning of a local replica of the authoritative FG.

The FG will use appropriate policies and procedures to determine with which entities it may peer.

Event Packages

The FGs SHALL support all required event packages in i3.[4]

Other General Requirements:

Proposers SHALL describe how they meet the following criteria:

[4] See NENA i3 at section 2.4.

- The FG SHALL accept coverage regions (civic and geodetic) from state-level and other authorized trees.
- The FG SHALL be provisioned with the coverage areas of all available trees. For example, in the end state, the U.S. FG will have at least 50 state trees plus additional state-level trees, while during transition, some states or state level regions may lack state or state-level trees, with county or other sub-state-level regions operating trees and injecting coverage regions into the FG.
- The FG SHALL accept the coverage areas of other trusted national FGs.
- The FG SHALL peer the urn:service:sos level with other FGs including service provider private replicas.
- The FG Operator MAY additionally offer to host private replicas on behalf of service providers, etc., that need national coverage, and MUST provide the ability for operators to provision a local replica.
- The FG SHALL receive both civic data structure (set) and a GML polygon (set) representing the coverage regions of the LoST trees. These coverage regions SHALL be received by the FG from the authoritative root node ECRF and LVF in each of the trees or from another FG.
- LoST-Sync SHALL be the supported mechanism for the exchange of information between trees and the FG and between FGs.
- LoST-Sync's <pushMappings> and <pushMappingsResponse> SHALL be the method for trees to provision coverage areas to the FG. See RFC6739 for details.
- LoST-Sync MUST use HTTPS.
- The FG MUST support mutual authentication for connections to it for query and/or publishing.
- The FG MUST utilize acceptable credentials, using policies and procedures approved by NIOC. At a minimum, acceptable credentials are traceable to the PCA.
- The FG MUST obtain a credential traceable to the PCA and use that credential for its side of TLS authentication.
- The FG SHALL require credentials traceable to the PCA for any entity authenticating to it, provided the querier operates in a role allowing it to make such queries of the FG.
- The FG SHALL allow for queries from entities without credentials traceable to the PCA, provided that it is not under stress, for purposes such as provisioning, LoST-Sync and service discovery by OSPs.
- The FG SHALL either provide credentials to authorized entities receiving LoST-Sync copies of its mappings or accept credentials traceable to the PCA.
- For FGs from countries that lack a PCA or operate a similar PKI with a different root, credentials from a trusted certificate authority are acceptable. NIOC SHALL approve policies and procedures for establishing which entities and credentials are acceptable for peering and coverage region injection, such as through cross-signing of root certificates across PKIs or explicit trust for specific trusted entities, such as a specific FG.
- The FG SHALL maintain logs detailing the transactions, including which entities (including its credentials) provisioned coverage areas and when the provisioning occurred.

Conformance with NENA-INF-009.1-2014

This RFP is intended to cover all requirements of NENA-INF-009.1-2014: Requirements for a National Forest Guide Information Document ("Forest Guide REQ").[5] However, all requirements of the FG REQ are

[5] Available at https://cdn.ymaws.com/www.nena.org/resource/resmgr/Standards/NENA-INF-009.1-2014_Forest_G.pdf.

considered normative in this RFP. The exception to this provision is where there is a conflict in requirements between both documents; where there are conflicts, this document prevails.

Optional Requirements

Proposers are encouraged to respond to the following optional requirements. While they will not directly impact scoring of responses to this RFP, NIOC and/or NENA may pursue engagements with proposers outside of this RFP based on responses to the options below.

Optional Requirement: Open Source Preference

Proposers are strongly encouraged to use open source solutions in their proposal, or if developing new code to provision the FG, to make available this code as open source. Proposers SHALL describe to what extent their existing solution is open source and SHALL also describe to what extent their solution will be made open source upon delivery of project deliverables. For those proposing to provide all or part of a solution as open-source, proposed shall explain how the proposed or extant governance model, such as conventions or standards for reviewing pull requests.

Optional Requirement: LoST-as-a-Service

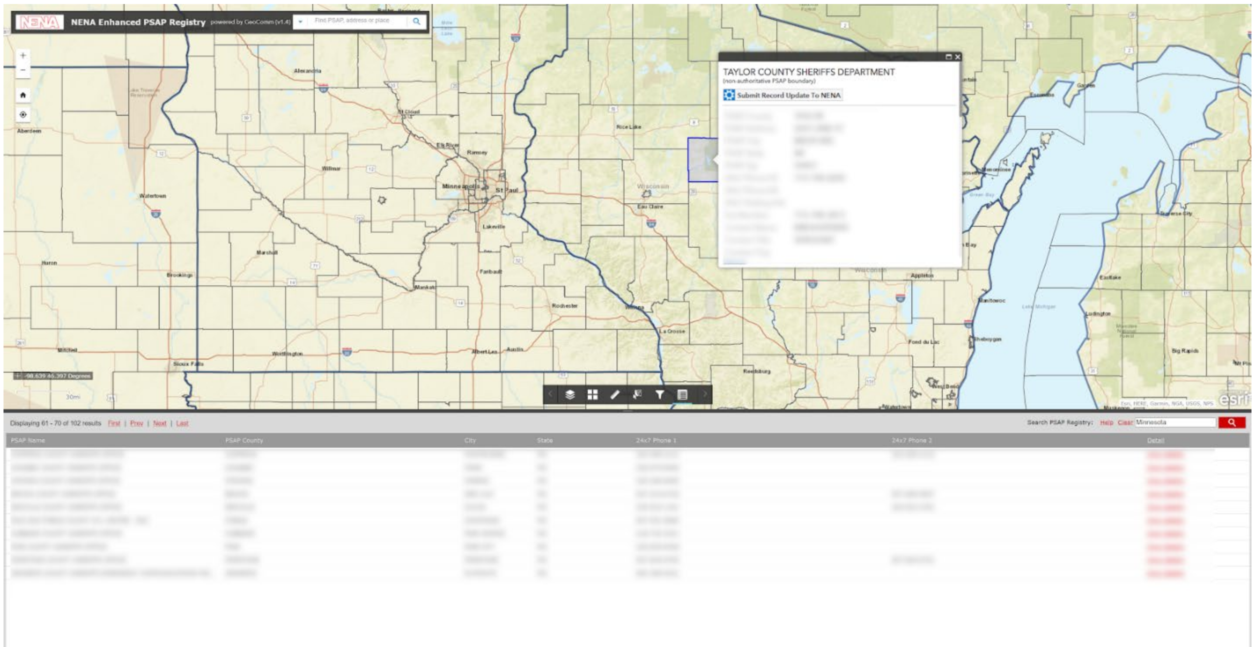
The FG operator MAY provide a LoST service for NG9-1-1 so that NG9-1-1 stakeholders, such as OSPs or ESInet operators, MAY leverage the services of the FG provider to operate a LoST server, such as an agency ECRF or LVF as-a-service. Proposers SHALL describe whether they will elect to provide this service, any associated costs and how the service SHALL be operated distinctly from the FG, regardless of any shared technology or provisioning procedures.

Optional Requirement: LoST/FG Test Service

It is strongly desired that the authoritative FG provides for a test service so that software developers, integrators and operators can test conformance with LoST and other protocols supported by the FG. Proposers SHALL describe whether they will provide such a test service, what this test service supports and any associated costs.

Optional Requirement: NENA EPRC Integration

It is strongly desired that the FG leverages synergies with the NENA EPRC, or Enhanced PSAP Registry and Census. The EPRC is a secure database, web portal and map that contains information about PSAPs throughout the United States. This central database will continue to fulfill the NENA PSAP Registry's original purpose of supporting PSAP and 9-1-1 Authority personnel to locate and contact other PSAPs during critical transfer situations.



TAYLOR COUNTY SHERIFFS DEPARTMENT
(non authoritative PSAP boundary)
Submit Record Update To NENA

Displaying 61 - 70 of 102 results First | Prev | Next | Last

Search PSAP Registry: Help Clear Minnesota

PSAP Name	PSAP County	City	State	24x7 Phone 1	24x7 Phone 2	Detail
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]

Figure 7: NENA EPRC

The EPRC is hosted on an ArcGIS Server and includes a feature layer that contains operating boundaries for PSAPs in the United States. Service area polygons include a variety of information about PSAPs in their attribute tables, including transfer numbers, address, administrative contacts and others. These service areas are non-authoritative at launch and are being updated to reflect authoritative service areas for PSAPs over time.

While the EPRC is not intended to perform routing for live 9-1-1 calls in the United States or elsewhere, that NENA operates a geospatial data set reflecting the service areas of US PSAPs has clear implications in the context of this RFP. As of this writing, the EPRC does not contain any LoST query information and accordingly is not capable of performing call routing; however, it does contain 24x7 call numbers for call transfers, which is its primary purpose. For example, the FG MAY provide a response from EPRC records if the LoST query fails to resolve (i.e., no service available at this location), such as the 24x7 transfer-to number. The EPRC supports location-based and other queries per ArcGIS Server's commercial API. Accordingly, Proposers SHALL describe the following:

- Whether the proposal is capable of integrating with the EPRC, and how, such as updating FG service area boundaries based on authoritative EPRC boundaries OR updating EPRC data based on authoritative boundaries provisioned in the FG
- Considering that EPRC does not support LoST-Sync and rather uses Esri's native API, what work would need to be done so that EPRC supports LoST-Sync, or at a minimum, what translations the FG MAY need to make in order to be compatible with the API.
- What value the EPRC MAY have in the FG query or provisioning chain, if any.

Note that any such integration with the EPRC SHALL be financially accounted for separately and distinct from any FG interactions and MAY be under a separate contract with NENA and certain aspects of such integration MAY not be subject to oversight by NIOC.

Transitional Characteristics

- During the transition to NG9-1-1, the FG SHALL be capable of supporting geographies that are not NG9-1-1 ready. If the FG determines that the location queried is in an area that is not represented in the FG (as opposed to a location that is not valid but is within a known coverage area), it will return new error condition of "NG9-1-1 Service not implemented". To facilitate the recognition of these "uncovered" areas, the FG SHALL establish a transitional root node ECRF that contains all of the uncovered areas for the FG's footprint.
- During transition to NG9-1-1, the internal FG may receive queries from clients other than an authorized provisioning tree and SHALL have the right to refuse queries if the FG is under stress. The FG can change its policy on responding to queries from entities other than authorized provisioning trees at any time, for example, when under stress from any load beyond its nominal capacity.

Operational Requirements

The FG is crucial for inter-agency call delivery. Service levels and availability minimums MUST be documented and enforced to ensure that call routing can occur between geographic domains covered by different LoST trees. Without a functional and reliable FG, each state-level area risks isolation and is potentially unable to determine routing for locations outside its jurisdiction. . This is exacerbated during the nationwide transition to NG9-1-1 because some areas will lack a statewide LoST tree; there may be sub-state-level regions that establish their own ESInets and LoST trees. Absent a state-level LoST tree, these regions are likely to rely on the national FG to route calls between them. Potentially, absent a well-functioning national FG, a county might be unable to transfer calls to its neighboring county since they are in different LoST trees.

Originating service providers may choose to deploy internal replicas of the national FG, and so may peer with the national FG in order to maintain accurate mappings.

The CONTRACTOR, in conjunction with NIOC, needs to provide for technical oversight capabilities and support. This includes determining where FG node clusters are located, which entities/persons have physical access and network access, which administrative or other capabilities they have, backup requirements, etc.

Proposers SHALL describe how they will support such administrative and technical oversight as part of their service offering.

Security and Resiliency

The FG is a critical component that is relied on during the processing of some emergency calls.

The FG SHALL be capable of withstanding the largest feasible DDoS/TDoS attack. The i3 specification notes that that means at least approximately a terabit of mitigation. As noted in i3, network, firewall/border control bandwidth as well as mitigation services may be used to achieve this requirement. As noted in i3, DDoS/TDoS mitigation typically requires that traffic be rerouted to a mitigation service. Private connections SHALL be able to be re-routed in this way if mitigation is needed.

The FG SHALL be operated in accordance with best practices for critical public network infrastructure. Proposers SHALL describe how they will support such oversight as part of their service offering.

Authorizations

The FG needs to be operated using policies and procedures developed or approved by the NIOC. These include determining which authorities are responsible for which regions and thus may use LoST-Sync or the SI to add or update coverage regions, with which entities the FG may peer, etc.

The CONTRACTOR SHALL establish a process, with the approval of the NIOC, for requests for new trees wishing to publish their coverage to the FG. The process MUST include identity and credential verification to assure that only appropriate 9-1-1 Authorities are approved to provide coverage information to the FG. Where higher level authorities publish data to the FG, the FG should, as much as possible, discourage listings by lower level agencies in a state or region.

The CONTRACTOR may establish an appeal process for trees with gaps and overlaps that are not resolved by mutual agreement among the affected parties.

Proposers SHALL describe how they will support such authorization as part of their service offering.

Availability

When under stress, the FG may need to prioritize certain operations over others. The priority of the supported interfaces is:

- Internal FG ECRF queries (civic and geospatial);
- External FG ECRF queries (civic and geospatial);
- Internal FG Lost-Sync requests (civic and geospatial);
- External FG Lost-Sync requests (civic and geospatial);
- Internal FG SI requests;
- External FG SI requests;
- Internal FG LVF queries (civic and geospatial);
- External FG LVF queries (civic and geospatial).

The objective for any implementation is to have availability of a FG 99.999% of the time, per best practices in provisioning public safety services. Proposers SHALL meet the following availability for the authoritative FG to be operated by the CONTRACTOR. Additionally, proposers SHALL describe how provisioning local replicas of the FG allows for an aggregate of 99.999% availability across the authoritative and replica FGs for responding to queries, and 99.99% availability for provisioning.

Availability for the authoritative FGs is defined for four sets of services:

Accepting and responding to queries:

- The internal FG SHALL have 99.99% availability 24/7.
- The external FG SHALL have 99.9% availability 24/7.
- The internal FG SHALL respond to a <findService> request within 50 milliseconds at least 99.99% of the time during any 30-day period.
- The external FG SHALL respond to a <findService> request within 50 milliseconds at least 99.9% of the time during any period.

Accepting and responding to LoST-Sync requests (<pushMappings> requests)

- Available 99.9% 24/7 for both the internal and external FGs.

Initiating LoST-Sync updates

- Available 99.9% 24/7 for both the internal and external FGs.

Accepting Spatial Interface (SI) requests

- Available 99.9% 24/7 for both the internal and external FGs.

Proposers SHOULD submit proposals that demonstrate the ability to exceed these availability metrics; these are the lowest acceptable availability metrics that constitute an acceptable proposal. Proposers SHALL demonstrate an architecture that can achieve very high availability (up to 99.999%) for a FG to be available to respond to queries, whether through a very high availability (99.999%) authoritative FG; an architecture that assumes a high-availability replica (99.99% or 99.99%) and a high availability authoritative FG (99.99%); or some other approach.

Availability is measured from the perspective of clients with adequate connectivity. Availability is calculated monthly and on a rolling 12-month average basis. Proposers SHALL propose a method of measuring availability that represents the view of the service as seen by the trees, not counting the network connecting the ECRF or LVF to the FG or the ECRF/LVF itself.

Maintenance, upgrades, etc. SHALL be performed so as to not impair availability or performance of <findService> queries. Availability or performance of other interfaces and requests may be degraded during approved maintenance or other servicing windows but SHALL not be below 99% during the window.

Subject to NIOC approval, the CONTRACTOR SHALL establish a pre-scheduled weekly maintenance window. The CONTRACTOR SHALL issue a notice to an email list maintained by the CONTRACTOR 30 days in advance of any planned maintenance within the pre-scheduled maintenance window that has a reasonable probability of causing a failure noticeable by clients of the FG. Maintenance activity outside the pre-scheduled maintenance window is permitted but requires the same 30-day notice as well as prior approval by the NIOC. Emergency maintenance may occur outside a scheduled maintenance window ONLY when required to repair an active or impending failure, or to correct a significant security vulnerability. All emergency maintenance MUST be preceded by an email announcement clearly labeled as an emergency maintenance notice. As noted above, the FG SHALL be deployed such that <findService> queries are not impaired during maintenance windows.

The CONTRACTOR SHALL perform a Root Cause Analysis for any failure of the FG that was, or could have been noticed by a client. The RCA report SHALL be shared with the NIOC and completion of follow up actions required to eliminate the same failure from recurring SHALL be communicated to the Board.

The CONTRACTOR SHALL deploy the FG functional element in a geo-diverse manner so that there is no single point of failure.

The CONTRACTOR SHALL provide 24x7x365 support. The CONTRACTOR SHALL establish a ticketing process to track problem reports, which MUST be accessible to all authorized users of the FG. The source of the ticket (authorized user and agency) SHALL be able to grade the ticket with at least “Major impact to operations, minor impact to operations, no impact to operations”. Service Level Agreements MUST be offered specifying 1 to 2 hour response for major, 24 hour response for minor, and 7 calendar day resolution for no impact. “Response” might not include a full resolution of the problem, but if it does not then a committed plan for resolution MUST accompany the response. The CONTRACTOR SHALL issue a monthly report to the NIOC on tickets. The CONTRACTOR SHALL notify the NIOC within 24 hours of any Major ticket (or within 2 hours if the service availability SLA is violated).

Capacity

The FG SHALL have the capacity to serve 100 simultaneous <findService> queries, and 100 simultaneous other queries and interface requests. Both the internal and external FGs SHALL be capable of maintaining sufficient coverage regions in each region type (ECRF civic, ECRF geospatial, LVF civic, LVF geospatial) to cover the whole of the United States, as well as sufficient coverage region to sync with at least 8 FGs in each of the following continents/regions:

- The United States and Canada
- North America other than the United States and Canada
- South America
- Western Europe (EENA and EU member countries and the UK)
- Europe (non-EENA and non-EU member countries and not the UK)
- Middle East (portions of Africa and Asia)
- Africa
- Central Asia
- East Asia
- South Asia
- Southeast Asia
- Australia
- Other

Reports

The CONTRACTOR SHALL issue a monthly report to the NIOC containing:

- The number of coverage regions in each of the four region types, for both the internal and external FGs. The report SHALL highlight discrepancies (if any of the eight types have more or fewer coverage regions).
- Gap areas within the U.S. (areas not contained in any coverage region) greater than TODO meters in area.
- Overlap areas within the U.S. greater than TODO meters in area.
- Monthly and daily mean uptime during the month.
- Service outages during the month (time and date of occurrence and duration).
- Trouble Tickets received, cleared, average clearance time, worst case clearance time.
- Discrepancy Reports received, cleared, average clearance time, worst case clearance time.
- Discrepancy Reports generated.
- The CONTRACTOR SHALL provide timely error reports to the Sponsoring Entity and all contributing tree nodes.
- The CONTRACTOR SHALL track the aging of errors and provide periodic reminders to contributing nodes of outstanding errors. A summary of these errors SHALL be reported monthly to the Sponsoring Entity.
- The CONTRACTOR may provide a method for conveyance of potential errors to the contributing nodes. This may include the downloading of coverage area overlaps.
- The CONTRACTOR SHALL issue a narrative report yearly that summarizes operations for the year, suggests changes to operation or oversight activities, processes or procedures and summarizes costs and projected pricing for the upcoming year.

Gap/Overlap

As coverage regions for state level trees are provisioned or injected (using SI or Lost-Sync) into the FG, the FG checks if any coverage regions overlap more than a configured threshold, and if there are gaps between regions that are within a configured range, that is, larger than a gap ignorance tolerance maximum size configuration, and smaller than a missing region minimum size configuration. Especially during the transition to nationwide NG9-1-1, there might be state level regions that do not have state level ESInets, LoST trees, etc., although sub-state level regions within the state level region might have their own ESInets, LoST trees, etc. The FG needs to be able to ignore large gaps that result from uneven deployment of NG9-1-1 while alerting to gaps that indicate configuration problems that can be corrected, along with overlapping coverage regions that likewise can be corrected.

The NIOC will establish policies for the size thresholds for gap and overlap processing. Gaps and overlaps within the alerting thresholds SHALL cause notification using the GapOverlap event as defined in STA-010.3.

Upon provisioning or injection of coverage regions, the provisioning tree node SHALL be notified of errors and warnings using the GapOverlap Event defined in NENA STA-010.3.

- The FG MUST report gaps and overlaps within the provisioned range. To do so, it uses the GapOverlap event.
- Tree Node Authorities who provide source coverage areas to a FG MUST subscribe to the FG's GapOverlap event.
- The event notifies both agencies when it receives data that show a gap or overlap within the provisioned range. The notification includes the layer(s) where the gap/overlap occurs, whether it is a gap or an overlap, and a polygon that represents the gap or overlap area.
- The FG may reject an update to a tree coverage area until errors are resolved. Until the issue is resolved, any previously provisioned coverage area will remain in effect.

Proposers SHALL explain the expected time between updating a GIS layer and provisioning into the FG to validate overlap, as well as their workflow.

The GapOverlap Event SHALL contain the following elements:

Table 1: GapOverlap Event

Element	Condition	Description
Agency	Mandatory	URI of Agency with gap/overlap. Will be repeated at least twice
Layer	Mandatory	Enumeration of layer where gap/overlap exists. May occur multiple times
Gap	Mandatory	Boolean, True if gap, false if overlap
Area	Mandatory	GML Polygon area of gap/overlap

- Civic data structure errors SHALL include:
  - Invalid, duplicated, or missing civic data structure elements
  - For tree nodes, civic data structures that are not defined below the Country level.
- Overlaps at the A1 + A2 (the combination of state and county) level or higher.
  - In the event that more than one contributing node contains the same combination of A1 + A2 + A3, the FG SHALL provision all sources and subsequently choose any one for a response to a query.
- Polygon data structure errors SHALL include:
  - Malformed message.
  - Empty or invalid geometry.
  - Transaction not authorized.
  - Gaps within a specified size threshold (see GapOverlap Event).
  - Overlaps larger than a specified threshold (see GapOverlap Event)
- The FG SHALL maintain a list of authorized provisioning trees. This list is also used to determine which trees (ECRFs and LVFs) are allowed to query the internal FG when access is restricted.
- The FG SHALL report any errors with Lost-Synch <pushMappings> as specified in RFC 6739.

Business Model

NENA envisions that, after a startup period, the FG will be self-sustaining by charging for access to the FG. Until there are enough connections to the FG to sustain the program, NENA will finance the initial development and operation of the FG. Additionally, NENA expects to recover its initial investment in the FG through receiving a portion of fees charged to access the FG; once NENA's investment has been recovered, NENA will reduce its fee collection to only the minimum level required to cover the administrative cost of administering the contract for the FG.

The FG SHALL be operated with a revenue-neutral mandate, with oversight by the NIOC.

Proposers SHALL include a business model addressing at least the following:

- CAPEX for establishment of FG
- OPEX for operating the FG
- A proposal for how fees should be assessed to support the operation of the FG
- A commitment to NIOC's "open books" financial policies; meaning, total expenses reimbursed to the operator SHALL be public knowledge
- Proposers SHALL include a separate and distinct business model for each optional requirement included in the proposal, as appropriate.

Evaluation of Proposals

Bids will be evaluated by a NIOC and/or NENA team using the following criteria out of a total of 100 points:

Table 2: Evaluation Criteria

Criterion	Points
Technical quality of the proposed solution	20
Conformance with the Requirements of this RFP	15
Prior experience in operating NG9-1-1 core services, ESPECIALLY LoST/ECRF/LVF functions	15
Participation in relevant NENA and/or IETF standards development by project principals	10
Ability of the offeror to provide detailed plans for how interoperability with other FGs will be achieved	10
Total Cost[6]	30
Optional Requirements	0

RFP Mechanics

NIOC

As specified throughout this section, all activities performed by NENA are subject to oversight by the NG9-1-1 Interoperability Oversight Commission (NIOC). NIOC is responsible for overseeing and approving all contract actions including the option to directly participate in the procurement process. NIOC may, at its discretion, direct NENA in whole or in part to manage the procurement, with or without direct supervision of one of more NIOC officers, at its discretion. The final proposal will be approved by NIOC, per recommendation from NENA, should NIOC direct NENA to do so. Accordingly, where named below, NENA means either “NENA”, “NIOC”, “NENA and/or NIOC” and/or “NENA under NIOC oversight and/or direction”. The direction and/or oversight provided by NIOC SHALL be made at a meeting generally open to the public and SHALL be clearly reflected in NIOC’s meeting minutes and in a press release at its public website (https://ng911ioc.org).

Contract Terms

NENA will enter into a contract with a RESPONDENT (the CONTRACTOR) who will be responsible for the performance of the services associated with operating the services described in this RFP, including full

[6] As the FG has a revenue-neutral mandate, proposers are DISCOURAGED from proposals that generate excess revenue for NIOC and NENA; such proposals will be scored lower than proposals that represent better value to the 9-1-1 community.

implementation of the services and any necessary hardware or software, on behalf and upon approval of the selected vendor by NIOC. After completion of the implementation of the services associated with this RFP, the CONTRACTOR will be responsible for continued services, maintenance and ongoing support. The CONTRACTOR will be the sole point of contact with respect to all contractual matters, including any and all contract performance issues and obligations. Additionally, CONTRACTOR is responsible and accountable for all obligations subcontracted to a subcontractor or third party.

RESPONDENTs may partner with third party subcontractors provided that all proposals on behalf of multiple vendors must be consolidated into a single proposal and identify a single RESPONDENT as the "RESPONDENT" and all other vendors as "subcontractors." Subcontractors proposed to provide a substantial part of the service MUST be identified in the proposal. A RESPONDENT may only act as a RESPONDENT for one proposal. A single RESPONDENT may be named as a subcontractor on multiple proposals submitted by other RESPONDENTs. Only one contract (and not a series of separate contracts) will be entered into between the Agency and the successful CONTRACTOR. The CONTRACTOR must ensure that appropriate contractual relationships are established with all subcontractors.

The Apparent Successful RESPONDENT will be expected to enter into a contract. NENA will evaluate RESPONDENTS based on the likelihood of reaching Contract terms that are fair and reasonable, based on the RESPONDENT'S responses to the terms of this RFP.

This RFP does not obligate NENA to contract for service(s) specified herein. If the contract is awarded, NENA reserves the right to make modifications to the original scope of work AND negotiate with the winning Apparent Successful RESPONDENT on the final costs, terms and conditions of the contract.

NENA will not be liable for any costs incurred by the RESPONDENTs in preparation of a proposal submitted in response to this RFP, in conduct of a presentation, or any other activities related to responding to this RFP.

NENA reserves the right at its sole discretion to reject any and all proposals received without penalty and to not to issue a contract as a result of this RFP. NENA also reserves the right in its sole discretion to waive minor administrative irregularities contained in any proposal.

All proposals will be reviewed by NENA under oversight by NIOC to determine compliance with administrative requirements and instructions specified in the RFP. Further, NENA MAY solicit volunteers from the 9-1-1 community, under NIOC guidance, to review proposals. Only responsive proposals that meet the minimum requirements will be forwarded to the evaluation team for further review.

NENA reserves the right to waive minor administrative irregularities contained in any Proposal. Additionally, it reserves the right, at its sole option, to make corrections to RESPONDENTS' Proposals when an obvious arithmetical error has been made in the price quotation. RESPONDENTS will not be allowed to make changes to their quoted price after the Proposal submission deadline.

NENA may waive minor irregularities in a Proposal provided that, in the judgment of NENA, such action will not negate fair competition and will permit proper comparative evaluation of Proposals submitted. NENA's waiver of an irregularity will in no way modify the RFP documents or excuse the RESPONDENT from full compliance with other RFP requirements.

RESPONDENTS are liable for all errors or omissions contained in their Proposals. RESPONDENTS will not be allowed to alter Proposal documents after the deadline for Proposal submission. NENA is not liable for any errors in Proposals. NENA reserves the right to contact RESPONDENT for clarification of Proposal contents.

In those cases where it is unclear to what extent a requirement or price has been addressed, the evaluation team(s) may, at their discretion, contact a RESPONDENT to clarify specific points in the submitted Proposal. However, under no circumstances will the RESPONDENT be allowed to make changes to the proposed items after the deadline stated for receipt of Proposals.

All Proposals received shall remain confidential and will not be disclosed by NENA.

Notice of intent to Respond and attendance at mandatory Pre-Bid Conference

A notice of intent to respond and attend the Mandatory Pre-Bid Conference must be received by NENA from the RESPONDENT no later than as indicated in the Schedule of Activities. This intent is transferrable to any of the RESPONDENT's successors; it is acceptable for a RESPONDENT to submit a notice of intent and later form a partnership with a third party that did not.

RESPONDENTS shall be accorded fair and equal treatment with respect to any opportunity for discussion or communications about their Proposal. This RFP is being conducted as a competitive solicitation NENA will not schedule meetings with any potential RESPONDENT except as set forth in the RFP and the procurement schedule. Once Proposals are submitted, NENA will communicate with RESPONDENTS only for the limited purpose of clarifying such factors as may be necessary for NENA to determine the Apparent Successful RESPONDENT. Discussions may be conducted with RESPONDENTS for the purpose of clarification to assure full understanding of, and RESPONDENT responsiveness to, the RFP requirements. NENA may request meetings with RESPONDENT for this purpose. In conducting discussions, there shall be no disclosure of any information derived from Proposals submitted by competing RESPONDENTS.

Some opportunities for dialogue between NENA and RESPONDENTS have been structured into the RFP schedule, including oral interviews, presentations and opportunities for RESPONDENTS to pose questions and get answers from NENA. NENA may, at its discretion, conduct additional communications with RESPONDENTS to clarify Proposals, or to respond to information relating to relevant past performance. All these communications, whether oral or written, will be referred to as "discussions." Any discussions may not be used to change the terms or specifications of a Proposal or to solicit such changes. Such discussions shall not be used to cure Proposal deficiencies or omissions, alter the technical or cost elements of the Proposal or otherwise revise the Proposal. Discussions may be used to eliminate minor irregularities, informalities or apparent clerical mistakes in the Proposal.

A Mandatory Pre-Bid Conference will be held on the date shown in the Schedule of Activities. The purpose of the Mandatory Pre-Bid Conference is to provide additional insight into NENA's goals for this procurement, provide updated and/or additional information regarding the requirements of NENA or the procurement process, and to provide RESPONDENTS with an opportunity to ask questions and/or provide feedback to NENA regarding the specifics of the RFP - including the structure, processes, functionality, requested/available technologies, and content.

All qualified RESPONDENTS interested in bidding are required to attend this conference in person or by conference call.

All questions RESPONDENTS have after the pre-bid conference must be submitted via email, and are due by the date indicated in the Schedule of Activities. Submissions will be directed to the RFP Coordinator at rfp@ng911ioc.org or as otherwise indicated at NIOC's website (https://ng911ioc.org). NOTE: No verbal inquiries will be accepted.

The questions asked, whether, in the Pre-Bid conference or received by NENA by email prior to the above date, and the subsequent answers provided, will be distributed in writing to all RESPONDENTs.

Notice of intent to respond to this RFP and attend the mandatory conference must be sent by email to NENA, directed to the RFP Coordinator.

E-mails provided for this conference shall include the company name, contact name and title, complete address, e-mail address, fax/phone numbers and will also list the names and contact information of any personnel attending, up to a maximum of three (3) attendees per RESPONDENT.

Your e-mail to NIOC will generate three actions –

- You will be added to the list of attendees.
- You will also be added to the potential RESPONDENT's e-mail list to receive any subsequent updates or amendments to the RFP (as they are made available)
- A non-disclosure agreement (NDA) will be prepared to codify NENA's intention to not disclose information in any bids received for this RFP.

Receipt of a request for attendance at the Mandatory Pre-Bid Conference is deemed confirmation of the RESPONDENT's receipt and review of the RFP, and acknowledgement of the requirements contained therein. Only qualified RESPONDENTs need attend the Mandatory Pre- Conference.

NDAs will be signed by NENA prior to the conference.

RESPONDENTs MAY elect to engage in a partnership following the mandatory pre-bid conference or to engage additional subcontractors following the conference. RESPONDENTS will not be prohibited in engaging in such arrangements so long as such arrangements are not anti-competitive in nature (subject to NIOC's determination) and/or violate any anti-trust laws of the United States.

Questions

Questions raised at the mandatory pre-bid conference and any answers provided at the meeting will be recorded by NENA. RESPONDENT'S questions regarding this RFP not raised at the conference will be accepted in writing via email on or before the date shown in Schedule of Activities above. Early submission of questions is encouraged. RESPONDENT'S questions must be submitted to rfp@ng911ioc.org or as otherwise indicated at NIOC's website (https://ng911ioc.org).

Only RESPONDENTS that submit questions by the due date and time specified above will receive a response to their questions. A RESPONDENT'S Subcontractors may only submit questions through the RESPONDENT'S question submission. RESPONDENTs should ensure that their questions are clearly stated as NENA will only answer the question as submitted and will not seek further clarity of the question being asked.

Written responses to all RESPONDENT questions, whether received at the pre-bid meeting or via email, will be posted and distributed to all RESPONDENTs without identifying the RESPONDENT posing the question. NENA will respond to all questions in writing by on the date shown in Schedule of Events below. No other form of posing questions and receiving responses from NENA will be allowed.

RESPONDENTS will use the following format when submitting their written questions:

Table 3: Q&A Template

Question #	Document Name	Section # and Title	Page or Paragraph#	Question

Questions are strongly preferred to be sent in Microsoft Office Word or Excel format (.docx or xlsx).

Proposal Format and Delivery

The proposal is to be sent to NIOC at rfp@ng911ioc.org or as otherwise indicated at NIOC's website (https://ng911ioc.org). NENA must receive all proposal responses no later than the date and time shown in the Schedule of Activities.

Late proposals will not be accepted and will be automatically disqualified from further consideration.

The proposal, in its entirety, must be delivered to the RFP Administrator in the form of a single PDF file containing all required and optional content EXCEPT the Price/Fee proposal, and a second PDF file containing only the Price/Fee proposal.

The files must be delivered electronically as identified in NENA's announcement on its website.

RESPONDENTs must clearly label all Proposals with the RFP Title: "Forest Guide Request for Proposals" and RESPONDENT name.

All materials submitted in response to this procurement become the property of NENA. Proposals received after the submission due date and time will not become the property of NENA and will be returned to the RESPONDENT. NENA will not own the underlying intellectual property rights (e.g., trademarks, patents or copyright) contained in the Proposals submitted in response to this procurement.

Responses to each question or request for information in the proposal should appear in the order presented in this RFP with the same headings used herein. This will not only be helpful to the evaluators of the proposal but should assist the RESPONDENTS in preparing the response.

Figures and tables must be numbered and referenced in the text of the Proposal by that number.

Failure to provide any requested information in the prescribed format may result in disqualification of the RESPONDENT. The RESPONDENT is specifically notified that failure to comply, or failure to provide a viable alternative in the judgment of NENA, with any mandatory part of the RFP will result in rejection of the proposal as non-responsive.

Responses must be based only on the material contained in this RFP. The RESPONDENT is to disregard any previous draft material and any oral representations it may have received. All answers to the requirements of this RFP must clearly state how the requirement is met.

NENA reserves the right to revise the RFP and to issue amendments and addenda to the RFP. NENA also reserves the right to cancel or reissue the RFP in whole or part, prior to the execution of a contract. In the event it becomes necessary to revise any part of the RFP, amendments/addenda will be provided to all those who provided an intent to respond and attended the mandatory pre-bid conference. Amendments to the work plan, if any, shall be at the sole discretion of NENA.

NENA reserves the right to make an award without further discussion of the proposal submitted. Therefore, the proposal should be submitted initially on the most favorable terms that the RESPONDENT can propose. The RESPONDENT must be prepared to accept this RFP for incorporation into a contract resulting from this RFP. Contract negotiations may incorporate some or all of the RESPONDENT'S proposal. It is understood that the proposal will become a part of the official file on this matter without obligating NENA.

Required Content

The submitted proposal must be formatted as described above and include a Letter of Submittal, an Executive Summary, a Management Proposal, a Technical Proposal, References and a Price/Fee Proposal. The RESPONDENT must provide clear, concise, direct, detailed and specific responses to each item.

The seven (7) required sections include:

Letter of Submittal, including signed Certifications and Assurances

A Letter of Submittal including certification and assurance, signed and dated by a person authorized to legally bind the RESPONDENT to a contractual relationship; e.g., the President or Executive Director if a corporation, the managing partner if a partnership, or the proprietor if a sole proprietorship. Each RESPONDENT must indicate in the letter of submittal, and as a condition of contract award, that they will provide proof of insurance from the RESPONDENT'S insurance carrier, outlining the extent of RESPONDENT'S liability coverage. The Selected RESPONDENT shall, at its own expense, obtain and keep in force, liability insurance during the term of the contract. The Selected RESPONDENT or shall furnish evidence in the form of a copy of the insurance policy at the time of signing of the contract by the RESPONDENT.

Executive Summary

Executive Summary should provide a general description of the RESPONDENT and the services they will provide.

Management Proposal

As part of the RFP response, RESPONDENTS shall include a proposal/summary of how services responsive to this RFP will be managed to ensure the requirements and service metrics identified herein shall be realized and maintained:

- Provide a description of the proposed project staffing/organization and how the team will be managed during the course of the project, including any subconsultants or subcontractors.
- State the name, the title or position, and telephone number of the individual who would have primary responsibility for the project resulting from this RFP.
- Disclose who within the firm will have responsibility and final authority for the work under the proposed contract.
- Name other individuals providing service on the project.
- Identify responsibilities and qualifications of staff who will be assigned to the potential contract and the amount of time each will be assigned to the project.
- Provide resumes for the named staff, which include information on the individual's particular skills related to the project, education, experience, significant accomplishments and any other pertinent information.
- Provide an organizational chart of your firm indicating lines of authority for personnel involved in performance of this potential contract and relationships of this staff to other programs or functions of the firm. This chart must also show lines of authority to the next senior level of management.
- State the business name, address, principal place of business, telephone number and fax number of legal entity or individual with whom contract would be written.

- Provide the names, addresses and telephone numbers of principal officers (President, Vice president, Treasurer, Chairperson of the Board of Directors, etc.).
- Specify the legal status of the RESPONDENT (sole proprietorship, partnership, corporation, etc.) and the year the entity was organized to do business as the entity now substantially exists.
- Include the Federal Employer Tax Identification number
- State the location of the facilities from which the RESPONDENT would operate.

Technical Proposal

In the technical proposal section of the bid, RESPONDENT shall provide detailed technical information on how it proposes to meet the requirements detailed in this RFP. The RESPONDENT shall include a proposed business model and proposed modifications to the Certificate Policy and proposed Certificate Practice Statement.

References

The RESPONDENT must provide references as outlined earlier in this RFP. The references must be from non-RESPONDENT related organizations and must clearly state the RESPONDENT's company name on the reference form and contact information for the reference. These references must be provided prior to the pre-bid conference to be held when indicated in the Schedule of Activities.

References must sent to the RFP Coordinator directly from the reference. References received from the RESPONDENT will not be considered. RESPONDENTS are encouraged to contact the RFP Coordinator to determine if this requirement has been met, as failure to receive the required references could be cause for disqualification.

Price/Fee Proposal

In the Price/Fee portion of their bid, RESPONDENTs are asked to propose a business model generally conformant with the plan envisioned as described above.

Schedule of Activities

The table below shows the anticipated dates for milestones in this procurement, on or before the hour of 23:59:59 ET on that date.

Table 4: Schedule of Activities

Event	Date
NIOC issues RFP	11/20/2020
Deadline for notice of intent to respond	01/6/2021
Pre-Bid Conference (VIRTUAL)	01/13/2020
RESPONDENTS Submit Questions	01/20/2021
NIOC Responds to questions	01/29/2021
RESPONDENT Submits Proposal	02/15/2021
Conduct interviews with Semi-Finalists	02/26/2021

Acronyms/Abbreviations, Terms and Definitions

All acronyms used in this document are listed below, along with any new or updated terms and definitions.

Table 5: Acronyms

Acronym	Description
AUS	Application Unique String
DoS	Denial of Service
DOT	U.S. Department of Transportation
ECRF	Emergency Call Routing Function
ESInet	Emergency Service IP Network
FCC	Federal Communications Commission
FG	Forest Guide
GML	Geography Markup Language
HTTPS	Hypertext Transfer Protocol Secure

LoST	Location-to-Service Translation
LVF	Location Validation Function
NIOC	NG9-1-1 Interoperability Oversight Commission
PCA	PSAP Credentialing Agency
PSAP	Public Safety Answering Point
SNI	Server Name Indication
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URN	Uniform Resource Name

Table 6: Terms Used

Term	**Definition**
Forest Guide (FG) Sponsoring Entity	The organization(s) that provides oversight and financing for a national Forest Guide.

Forest Guide (FG) Operator	The organization selected by the FG Sponsoring Entity to deploy and operate a national Forest Guide.
Internal ECRF	An ECRF instance that resides within and is only accessible from an ESInet instance
External ECRF	An ECRF instance that resides outside of an ESInet instance
Private Forest Guide (FG) Replica	An instance of the FG that is generally limited in access to entities that contribute coverage areas.
Public Forest Guide (FG) Replica	An instance of a FG that is accessible to any authorized entity