NEBRASKA

PUBLIC SERVICE COMMISSION

REQUEST FOR PROPOSALS

FOR EMERGENCY SERVICES IP NETWORK (ESInet) and NEXT GENERATION CORE SERVICES (NGCS)

Public Service Commission

300 The Atrium, 1200 N Street

Lincoln, Nebraska 68509

COMMISSIONERS:

ERIC KAMLER

CHRISTIAN MIRCH

TIM SCHRAM

KEVIN STOCKER

DAN WATERMEIER

Contents

Executive Summary

The following is a summary of this Request for Proposal (RFP), the bidding process, and the contractual process.

Services to be Provided

The Nebraska Public Service Commission ("NPSC" or "Commission") is issuing this solicitation for the purpose of selecting a qualified bidder or bidders to contract for the provision of an Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) to enable statewide delivery of Next Generation 911 (NG911). The selected contractor will design, implement, test, cutover, operate, and maintain the solution, provide 24×7 support and manage the transition from existing legacy and NG911 systems to the Contractor's NG911 solution.

Length of Contract

The term of the contract will be **five (5)** years commencing upon execution of the contract by the Commission and the vendor. The contract includes the option to renew for **ten (10)** additional **one-year** periods upon mutual agreement of the Parties. The Commission reserves the right to extend the period of this contract beyond the termination date when mutually agreeable.

Key information about this RFP

- **Proposals under this RFP are due March 24, 2026.**
- This Request for Proposal process will include a mandatory Solicitation Conference. Please see the Schedule of Events for the specific date and time.
- This RFP process will have written questions and answers (Q&A). Please see the Schedule of Events for the specific time period of the Q&A.
- All information provided by the Commission about this solicitation will be posted publicly to the DAS website: https://das.nebraska.gov/materiel/bidopps.html.
- Bidders **must** meet the minimum qualifications provided in Minimum Essential Qualifications section contained in the **Proposal Instructions**.
- All responses received regarding this solicitation may also be posted to the DAS website. In submitting, any vendor must request that proprietary information be excluded from the posting. The bidder must identify the proprietary information, mark the proprietary information according to state law, and submit the proprietary information in a separate file or section conspicuously named as "PROPRIETARY INFORMATION." For more information on this, please see **Proposal Instructions**, below.
- A Technical Matrix is included as Appendix B.

Overview of Request for Proposal Process

The Commission has established its own Request for Proposal process. This process is similar to the process conducted by the Department of Administrative Services (DAS) pursuant to the State Procurement Act, Neb. Rev. Stat. §§ 73-801 et seq., and those agencies that are subject to the State Procurement Act. While the Commission is not subject to the State Procurement Act for the purposes of services, it has chosen to issue a formal competitive solicitation and therefore will be following its own established procedure (contained in this RFP). DAS is not responsible for this RFP and should not be a point of contact for any questions.

The RFP is made of four main parts: the **Project Requirements and Scope of Work**, **Procurement Procedure**, **Proposal Instructions**, and a **Glossary**.

1. The **Project Requirements and Scope of Work** describe the services and deliverables to be completed by a contractor.
2. The **Procurement Procedure** describes how this RFP will be conducted.
3. The **Proposal Instructions** describes what must or should be contained in the proposals from vendors; and
4. A **Glossary** has also been included to define the terms used throughout.

Overview of Contracting Process

After an Intent to Award is issued, the Commission will work with the winning bidder to formulate a final Scope of Work, based on the Project Requirements and Scope of Work in the RFP and the bidder's response. The Procurement Procedure and Proposal Instructions will not be included in any final contract.

This final Scope of Work will harmonize any differences between the Project Requirements and Scope of Work and the bidder's proposal, although it may not expand upon the scope of the Project Requirements and Scope of Work nor provide the winning bidder with any chance to modify their proposal nor costs to achieve any kind of competitive advantage over other bidders. The harmonization process will only streamline the glossary, scope of work, cost proposal, and deliverables to ensure the Commission has clearly defined costs, contractual obligations, and deliverables.

Project Requirements and Scope of Work

Bidders should review these Project Requirements and Scope of Work and other sections below. Bidders should provide a response to this section consistent with the **Proposal Instructions**, below. This document, along with bidder's response, will be incorporated into the resulting contract from this RFP as described in the **Procurement Procedure**, below.

A. PROJECT OVERVIEW AND BACKGROUND INFORMATION

Background

Nebraska has been executing a statewide transition from Legacy 911 and Enhanced 911 (E911) to Next Generation 911 (NG911) since adoption of the State 911 Service System Plan in 2017. The State's 68 Public Safety Answering Points (PSAPs) are organized into seven regions. In each region, two PSAPs operate as hosts with separate primary equipment, providing mutual backup and overflow. Other PSAPs function as fully capable remotes connected to the hosts via regional IP networks. Regions are interconnected by a vendor-hosted statewide ESInet using a fiber optic ring with two geographically diverse out-of-state data centers, enabling real-time communications and failovers across PSAPs and regions.

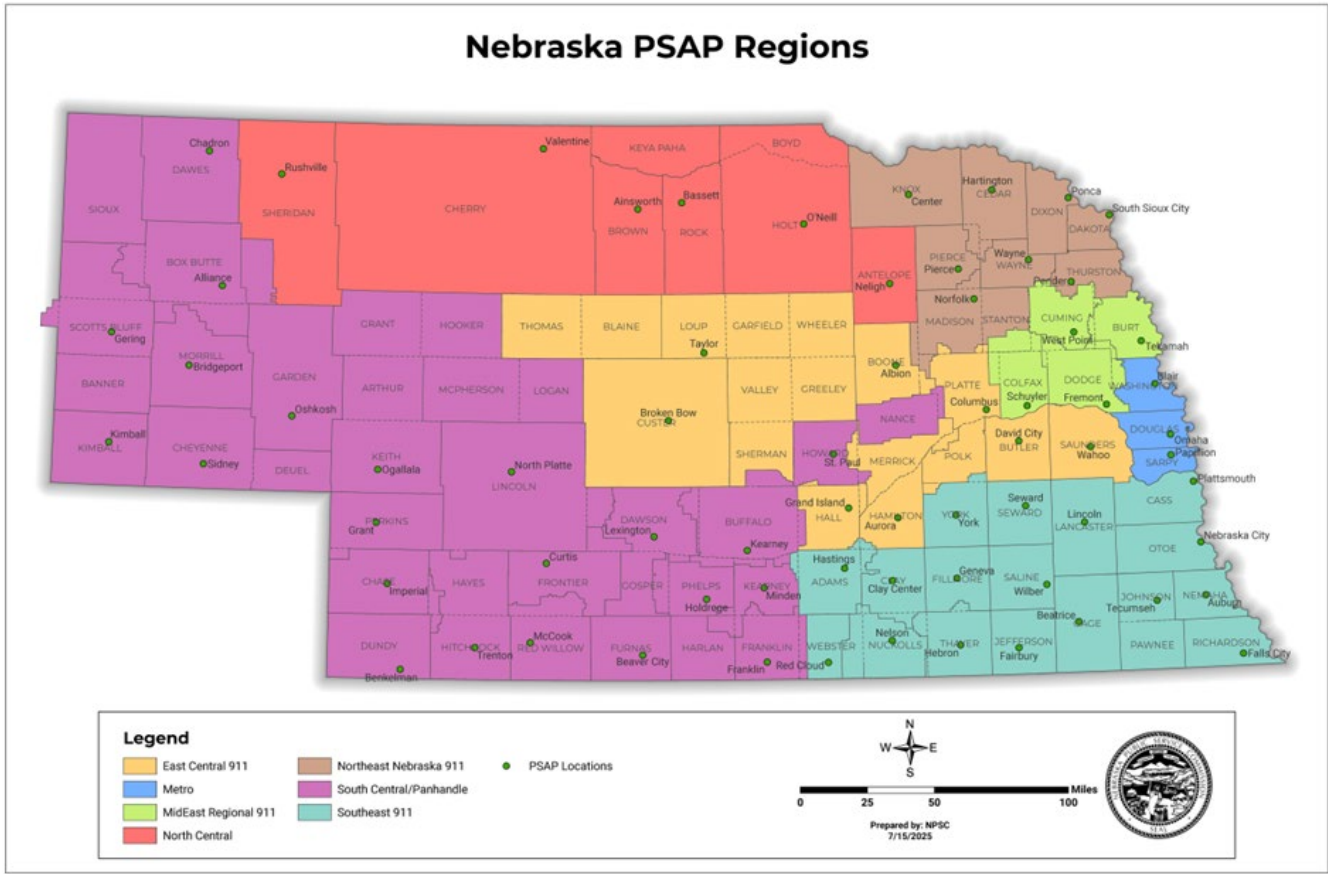


Figure 1: Nebraska PSAP Regions and PSAP Locations

The State's transition is driven by rising volumes of multimedia emergencies and the need to comply with evolving standards and rules for NG911. Recent developments (as of September 2025) include federal reliability expectations for NG911 networks and continued emphasis on accurate location and resilient operations. Nebraska's July 2025 initiative for NG911 data analytics and real-time reporting further underscores the State's focus on measurable performance and support for PSAP operations.

Project Overview

The State of Nebraska seeks a qualified Contractor to design, implement, operate, and support a statewide NG911solution that is fully conformant with the i3 Standard published by the National Emergency Number Association (NENA). This solution will include an Emergency Services IP Network (ESInet), Next Generation Core Services (NGCS), and all required hardware, software, and

integrations to serve the PSAPs statewide. It must interoperate with existing regional architectures, support secure and resilient call and media session delivery, and provide a clear migration path from currently deployed systems.

The system shall deliver high availability, security, scalability, and interoperability for NG911 communications, including voice, text, video, and data. To strengthen redundancy and reliability, the State requires one or more IP points of interconnect and prefers an in-state data center presence, while recognizing cost considerations and the need for flexible pricing and service options.

The Contractor will provide comprehensive operations and maintenance, including 24×7 monitoring, incident response, performance reporting, documentation, and compliance with applicable standards and policies. Service levels will be defined and measured to ensure continuity of operations, rapid restoration, and continuous improvement across all PSAPs.

Primary objectives include:

- Delivering a highly available, resilient ESInet and NGCS platform that meets applicable NG911 standards and State requirements.
- Enabling seamless interoperability among regions and PSAPs, with defined service levels and 24×7 operations and support.
- Providing a structured migration, testing, and cutover plan that minimizes risk and service disruption.
- Supplying performance monitoring, real-time reporting, and analytics to support operational oversight and continuous improvement.
- Ensuring security, privacy, and compliance aligned with applicable rules, with clear incident response and disaster recovery capabilities.

This procurement builds on Nebraska's statewide ESInet/NGCS environment that supports current needs and future NG911 capabilities.

2024 Call Counts

The following call counts are from the State's current 911 analytics platform.

Total 2024 calls: 954,264

- Wireless: 825,482
- Wireline: 47,878
- VoIP: 75,588
- Text: 5,316

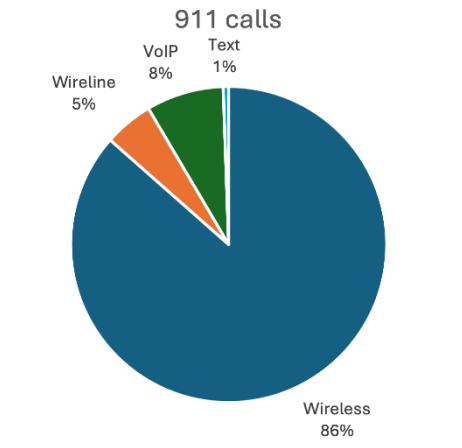


Figure 2: 2024 Nebraska 911 Call Statistics

Justification for the Proposed System

The current system's inefficiencies and NG911 failures justify a need for a refresh.

- **Regulatory Compliance:** Aligns with the FCC's 2025 NG911 rules for reliability and location accuracy.
- **Operational Improvements:** GIS-based routing reduces errors (including edge cases); multimedia support enables video for 20% of calls (e.g., VRS for Deaf, hard of hearing, and speech-disabled users).

- **Resiliency and Scalability:** Geo-redundancy addresses weather events and supports 150% of peak usage load.
- **Security Enhancements:** Mitigates terabit-scale DDoS attacks and applies zero-trust to counter rising cyber threats.
- **Cost Efficiency:** Phased migration minimizes disruptions; shared data centers optimize resources.
- **Future-Proofing:** Supports IoT, NG-AACN, and Emergency Incident Data Objects (EIDOs) and their conveyance between NG911 Functional Elements, positioning the system for conformance with NENA-STA-021.1-2021 and NENA-STA-024.1-2025 (and future updates). Full i3 conformance (e.g., REST/JSON interfaces) ensures interoperability with legacy environments.

Referenced Documents

- FCC Report and Order 13-158: 911 Reliability (with 2025 extensions for NG911 rules)
- ITIL v4: Service Management Practices
- Nebraska PSC NG911 RFP (July 2025): Reporting and System Requirements
- NebraskaMap GIS Datasets (2025 updates for NG911 boundaries)
- NENA-INF-008.2-2013: NENA NG9-1-1 Transition Plan Considerations Information Document
- NENA-STA-004.2-2024: NENA Next Generation 9-1-1 United States Civic Location Data Exchange Format (CLDXF-US) Standard
- NENA-STA-006.2-2022: NENA Standard for NG9-1-1 GIS Data Model
- NENA-STA-010.3-2021: NENA i3 Standard for Next Generation 9-1-1
- NENA-STA-019.2-2022: NG9-1-1 Call Processing Metrics Standard
- NENA-STA-021.1-2021: Standard for Emergency Incident Data Object (EIDO)
- NENA-STA-024.1.1-2025: Conveyance of Emergency Incident Data Objects (EIDO) between Next Generation (NG9-1-1) Systems and Applications
- NENA-STA-027.3-2018: E9-1-1 PSAP Equipment Standards
- NENA-STA-034.1-2022: NENA Legacy Selective Router Gateway (LSRG) Standard
- NENA-STA-040.2-2024: Security for Next Generation 9-1-1 Standard (NG-SEC)
- NENA-STA-046.3-2025: NENA Virtual PSAP Management Standard
- NENA-STA-049.1-202Y (Draft): NENA Transition to i3 PSAP Standard (Stable Form Notice issued October 2,2025)
- Project Management Institute PMBOK 7th Edition: Project Management Standards

Remainder of page intentionally blank

B. SCOPE OF WORK

Services to be Provided

The scope of this RFP encompasses the full lifecycle of the NG911 system, from design and implementation to operations and decommissioning. A comprehensive listing of the minimum technical requirements needed to operationalize a proposed solution is located in §E (Technical Requirements) of this document.

1. **ESInet Architecture and Design**
   - **a.** Contractor shall provide an ESInet design and implementation conforming to the NENA i3 ESInet architecture and functional requirements, including multi-site, geographically diverse redundant cores, session border control at boundaries, and tenant isolation. (This includes bandwidth provisioning, diagrams, availability, and reliability features).
   - **b.** Contractor shall support IPv4 and IPv6 addressing, implement Quality of Service (QoS) (DiffServ or equivalent) to prioritize emergency signaling and media, and document bandwidth and capacity needs for all services. (This includes referenced 99.999 requirements that will be included in the Service Level Agreement (SLA).
   - **c.** Contractor shall support SIP signaling per RFC 3261 and required NG911 SIP extensions (SIP over TLS for signaling, and SRTP for media, where used), and demonstrate SIP interconnects with external peers. (This includes SIP call flow across the ESInet, no calls "lost," and conversion where necessary).
   - **d.** Contractor shall provide documented peering and interconnect interfaces (LNG, LSRG, LPG, SBCs and other edge elements, Points of Interconnection) and APIs and procedures for peering with other ESInets and third-party providers. (Configuration management database, diagrams, IP schema).

2. **NG911 Core Services (NGCS)**
   - **a.** Contractor shall provide or interoperate with NGCS functional elements (BCF, ESRP, ECRF, LVF/LIS, MSAG/ALI-equivalent services, ESRP/ESRP-like routing proxy, etc.) as defined in the NENA i3 Standard and shall map which product components implement each NGCS function.
   - **b.** Contractor shall implement NGCS interfaces per the NGCS Interface Standard (SIP and REST interfaces, expected message formats including PIDF-LO where applicable) and shall provide interface documentation, schemas, and test harness endpoints.
   - **c.** Contractor shall meet stated latency and throughput SLAs for NGCS lookups and routing decisions. (99.999 from caller to call-taker unless specified in writing between the PSC and Contractor.)

3. **GIS and Location-Based Routing**
   - **a.** Contractor shall accept, store, and use GIS data in the NENA GIS data model/schema and SHALL maintain the required NENA layers (PSAP boundaries, ESN/service boundaries, address points, civic addressing, emergency routing attributes). GIS data shall conform to normative language identified in NENA-STA-006.2-2022. The Contractor may utilize NENA-REF-006.2-2023 (NENA NG9-1-1 GIS Data Model Templates) to assist in conformance to the Standard.
   - **b.** Contractor shall use authoritative GIS data for routing decisions (ECRF) and shall accept location in PIDF-LO format (and convert civic/geodetic input) for routing and display.
   - **c.** Contractor shall provide GIS data versioning, change tracking, import/export in NENA formats (e.g., GML/GeoJSON or NENA schema), and support automated incremental updates.

4. **Call Flow and Media Session Handling**
   - **a.** Contractor shall implement NENA i3 call flows (incoming SIP INVITE → ESRP/ECRF lookup → PSAP routing) preserving required SIP headers (P-Asserted Identity, Diversion, History Info, etc.) and shall deliver PIDF-LO location payloads with calls where required.
   - **b.** Contractor shall support real-time multimedia as defined by NENA (voice, IP text-to-911, real-time video, and supplemental data) with media negotiation, fallback behaviors, and preservation of metadata across transfers.
   - **c.** Contractor shall support PSAP call transfer (warm or attended and blind transfers) while preserving call metadata and location.

5. **Security, Privacy, and Trust**
   a. Contractor shall implement the NENA ESInet security and trust model including mutual TLS between NG911 elements, strong authentication and RBAC for administrative interfaces, and secure boundary elements (SBCs).
   b. Contractor shall encrypt sensitive data in transit (TLS 1.2+ / TLS 1.3) and at rest (AES-256 or equivalent), provide PKI/certificate lifecycle management, and protect cryptographic keys using a hardware security module or equivalent. Contractor shall support certificate revocation.
   c. Contractor shall provide incident response and vulnerability management processes and supply recent third-party penetration test reports and remediation plans.
   d. Contractor shall satisfy Neb. Rev. Stat. 86-125 by completing the affidavit provided by the State regarding the use of prohibited communications equipment by communications providers.

6. **Logging, Reporting, and Call Detail Records**
   a. Contractor shall produce end-to-end logs and Call Detail Records (CDRs) for every emergency transaction containing timestamps and share with the data analytics engine, correlation IDs, call identifiers, caller identity (if available), location used for routing, PSAP destination, media types, and call disposition.
   b. Contractor shall provide secure storage of logs and CDRs, role-based access controls, and export capability in open formats.
   c. Contractor shall provide operational reports (call volume, answer times, transfers, location failure rates, outage reports) and support ad-hoc queries.

7. **Interoperability, Testing, Conformance, and System Acceptance**
   a. Contractor shall participate in jurisdiction-specified interoperability and conformance testing, independent third-party validation and verification, demonstrate NGCS and ESInet interfaces in a test harness, and provide test results and logs.
   b. Contractor shall provide full product documentation, API specifications, training, runbooks, and operator and administrator manuals.

8. **Operational Support and Service Level Agreements (SLAs)**
   a. Contractor shall negotiate with the PSC to establish firm SLAs for availability, incident response, escalation, mean time to repair (MTTR), change management procedures, and maintenance windows.
   b. Contractor shall produce a rollback and contingency plan for major updates that affect routing/GIS or call handling.

Applicable Standards

Respondents must demonstrate their industry knowledge and describe their commitment to proposing standards-based NG911 solutions and services.

The State may disqualify or reject non-standard or proprietary systems that may hinder NG911 implementation, limit interoperability, or that might restrict the State from interconnecting to a regional or national 911 system in the future.

Throughout the duration of this contract, Respondents SHALL maintain conformance with all standards listed in this Scope of Work and ensure that the products, solutions, and services provided for the State of Nebraska evolve and adapt as the standards evolve. A listing of currently approved NENA standards can be found at https://www.nena.org/page/standards.

In their response, Respondents must explain in detail how their proposed solution conforms to the requirements of the referenced standards.

Federal Communications Commission Rules

The Federal Communications Commission (FCC) regulates 911 services through various rules and requirements, primarily found in **47 CFR Part 9**, covering Enhanced 911 (E911), Text-to-911, Next Generation 911 (NG911), and location-based routing. Key requirements include transmitting all 911 calls, providing call-back numbers and precise location data, ensuring service for text and multimedia, and meeting standards for digital, IP-based systems and network reliability.

Other Industry Standards

All equipment proposed to support or operate within the State of Nebraska NG911 System must comply with relevant industry standards and reference models, including, but not limited to:

- American National Standards Institute (ANSI)

- Electronic Industries Alliance (EIA)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- Open Systems Interconnection (OSI)
- Telecommunications Industry Association (TIA)
- Underwriters Laboratories (UL)

Respondents must propose a system that utilizes an Open Standards Methodology:

- The proposed system shall be subject to standards that enhance open standards and increase interoperability such as ITU, IEEE 802 at OSI Layer 2, and IP and TCP, as defined by the IETF in the applicable RFCs, at OSI Layer 3 and above.
- If proprietary standards or protocols are used within a proposed solution, Respondents shall disclose the proprietary nature and discuss any limitations that may result.

Conformance to Standards

Baseline Conformance

The State prefers full conformance with **NENA-STA-010.3** at System Acceptance. The solution must remain current with NENA standards as they evolve. The State understands some limitations may require additional development.

Gap Identification (Proposal Requirement)

Respondents shall identify any gaps to full **NENA-STA-010.3** conformance in their proposals. Respondents are solely responsible for disclosing such gaps and providing a plan and timeline to close them.

Note:

The State recognizes that no existing implementation fully conforms to NENA-STA-010.3 (and many still have gaps against NENA-STA-010.2). Proposals must explicitly state all areas where the delivered system will not conform at time of delivery.

Standards Updates (Post-Award)

Contractors shall implement any new or changed feature required by an upgraded or revised NENA standard **within nine (9) months** of the standard's ratification for public use. The Contractor must supply regular progress reports for features and functions that are in revision. If at any point in the 9 month window the Contractor becomes aware that they will not meet the deadline they must inform the State in writing with an adjusted timeline for when the new features or functions will be delivered. If the Contractor cannot meet this timeline, it must request a **waiver**, including an alternative plan and schedule to achieve conformance.

Non-Disclosure and Breach

Exceptions to conformance must be explicit. Notwithstanding any other provision in the contractual terms, if the system is delivered with a **material deviation** from **NENA-STA-010.3** that was **not** disclosed in the proposal, and the State determines (in its sole discretion) the omission was **not** accidental, the Contractor will be deemed **in breach** of contract. If the State determines the omission was accidental, the State and Contractor will negotiate in good faith a deadline by which conformance must be achieved.

Deviation Classification (Proposal Requirement)

Each deviation must be classified as one of the following:

- **NENA-STA-010.3 upgrade, proposed date:** The delivered system conforms for the feature, and the proposal includes an estimated date for providing the **NENA-STA-010.3** upgrade to the State (no later than **Contract Year 2**).
- **Missing capability, proposed date:** The delivered system does **not** conform to NENA-STA-010.3 for the feature; the proposal includes an estimated upgrade date (no later than **Contract Year 2**).
- **Missing capability, no proposed date (will be provided):** The delivered system does not conform to **NENA-STA-010.2** or **NENA-STA-010.3** for the feature; the proposal commits to provide the capability but does not specify a date.
- **Missing capability, no plans:** The delivered system does not conform and there is no intention to conform. An alternative to the **NENA-STA-010.3** feature may be proposed for State consideration.

Remediation Plan and Progress
Non-conforming features shall be listed in a **Remediation Plan** included with the proposal, identifying each feature and the estimated schedule. The Contractor shall update the Remediation Plan **at least quarterly**. The State expects reasonable, continuous progress. If any features remain non-conforming to **NENA-STA-010.3** by the end of **Contract Year 2**, the Contractor will be deemed **in breach** of contract.

Interoperability
The system must interoperate with any system conforming to **NENA-STA-010.3** that must interwork with the State's system. The State understands interoperability issues can arise from either party's non-conformance or from ambiguities in the standard. In such cases, the Contractor, the other vendor, and (as appropriate) the State's consultants shall work cooperatively to determine the non-conformance and corrective actions, using the **intent of NENA-STA-010.3** as the guiding objective.

- If the Contractor is required to make changes, it shall propose a completion date acceptable to the State.
- If the issue lies with the other vendor, the Contractor shall cooperate in testing but has no further responsibility.
- If the other vendor conforms to **NENA-STA-010.2**, the State's system conforms to **NENA-STA-010.3**, and the issue falls outside the **010.3** backward-compatibility statements for **010.2**, the Contractor is **not** required to make changes.

NENA NG911 i3 Standard Conformance
The following section includes references to conformance with **NENA-STA-010.3**. The absence of an explicit reference **DOES NOT** imply the State does not require conformance to that portion of the Standard. The State requires conformance to the full standard, while recognizing the practicalities of achieving conformance within the contract period as described above.

If the proposed system does not apply NENA Standards throughout the ESInet, the proposal must identify each deviation, explain why the Standard is not met, and propose an alternative.

Additional explicit Standards-conformance requirements appear in other sections of this RFP. **RESPONDENTS MUST COMPLETE THE STATUS TABLE** (Table 1) **BELOW.**

Status must be presented with one of the following options:

- **Implemented**
  - The requirement is tested, approved, and in production.
- **Roadmap – with timeframe in months**
  - The requirement is not in production for any reason.
  - **Timeline** for implementation **MUST be within 12 months** of RFP Response.
- **Future Planned**
  - The requirement is not in production for any reason, and the planned implementation is ***longer than 12 months***.
- **Not implemented**
  - The requirement is not in production, and no plans have been developed for deployment/implementation of the requirement.

Remainder of page intentionally blank

Table 1: NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

v3 Standard Requirements	What Does It Do?	**Status in Proposed Solution?** (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
ElementState and ServiceState	Allows a PSAP/State management app to see the status of each service (ESRP, ECRF (Emergency Call Routing Function)) and each "box" in a non-proprietary way	
All i3v3 interfaces plus i3v2 for backwards compatibility	REST/JSON interfaces conforming to i3v3 standard YAML with backwards compatibility to the i3v2 SOAP/XML interfaces	
Security Posture	Allows routing rules to take security state (green/yellow/orange/red) into account	
IPv6	Allows every element to have a public address and get calls/data from modern nets (wireless) without translation	
DNS based redundancy model	All services implement a redundancy model where more than one IP address is returned for the service URI, and any address can be used for a transaction	
History Info/Reason	Provides a logged reason why a call was not delivered the "normal" way	
Video	Supports video calls to 911. Most importantly, allows deaf callers using VRS to be seen by call takers. Includes BCF, Bridge and logging service support	
MSRP	Instant Messaging Service	
Non-Human Initiated Calls	Support for IoT devices, alarms, etc.	
TLS (Transport Layer Security) transport of SIP	Provides secure call signaling	
SRTP	Provides secure media (voice, video, text) for calls	
RTCP support on all SIP entities	Provides secure control of RTP (Real Time Transport Protocol) streams	
RTCP Extended Reports	Provides diagnostic information on media streams	

v3 Standard Requirements	What Does It Do?	**Status in Proposed Solution?** (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
PSAP detection of loss of RTP vs silence	Differentiates silent calls from mechanical loss of audio media stream	
Element Overload (RFC 7339)	Graceful coping with too many SIP calls	
STUN/TURN/ICE	Standards based mechanisms for NAT Traversal	
NG-AACN Support	Update to Automatic Car Crash Notification standards	
SIP Presence for location	Allows OSPs to send location updates for mobile devices without manual rebid (requires OSP to implement also).	
Policy Store i3v3 interface	Interoperable policy repository that allows 3rd party editors/verifiers/etc.	
Multiple Geolocation	Accepts more than one location reported in a 911 call	
Discrepancy Reporting mechanism + i3v3 defined DRs (Discrepancy Report)	Standardized way to report discrepancies with standardized responses	
Bad Actor mechanism	Allows PSAP to stop repeated bad calls from a source	
Call Suspicion mechanism	Allows the system to mark calls that MAY be bad, and then treat them specially at the PSAP (warnings, special queues, etc.)	
QueueState	Allows Policy routing based on queue congestion	
DequeueRegistration	Allows multiple PSAPs and other entities to dequeue from a queue	
ESRPnotify	Allows policy routing rule to notify some entity that a condition was encountered	
AbandonedCall	Standardized way to report a call that was hung up before PSAP got the call	

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Service/Agency Locator	Service that allows discovery of things on any ESInet rather than provisioning it.	
XACML based data rights management	Standardized way to control who has access to what data	
EIDO on Transfer	Mechanism to transfer call state to a PSAP along with the call	
3rd Party Origination	Allows a 3rd party, like Video Relay Interpreter, to be automatically added to a call as a 3 way	
RTT	Real Time Text support, includes multiparty RTT (Real Time Text) support (RFC 9071) and mixer support for non-aware devices	
Resource Priority header	Allows SIP Resource Priority handling of SIP messages. All SIP entities support it, BCF polices/inserts it.	
Incoming Baudot is converted to RTT	TTY to/from OSP converted to Real Time Text by LNG (Legacy Network Gateway) (Baudot to RFC 4103)	
Outgoing Baudot is converted to RTT	TTY to/from PSAP converted to Real Time Text by LPG (Legacy PSAP Gateway) (Baudot to RFC 4103)	
Multipart MIME (BCF, bridge, media server)	Allows multiple SIP bodies. Typically, this is Location by Value plus SDP.	
SRV records for SIP interface resolution (BCF/ESRP and PSAP)	Standard mechanism to derive SIP connection address from a domain name	
Support for Outbound (RFC 5626)	SIP Protocol fixes for outbound calls	
i3v3 Syntax and Semantics for Policy Routing Rules	Standardized Syntax and Semantics for Policy Routing Rules	
SBC inserts NENA-Source parameter	Allows PSAP to identify which SBC (BCF component) handled a call. Used with Bad Actor	
ESRP supports AdditionalData dereference for PRR	Allows policy routing based on additional data	

v3 Standard Requirements	What Does It Do?	**Status in Proposed Solution?** (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
ESRP handles incoming admin calls	Allows policy routing of admin calls	
ESRP policy routes calls to other agencies	Allows calls to other PSAPs, responders, to be policy routed. Includes extraction of location from an EIDO	
Support for incoming identity validation	STI-VS implemented to return STIR/SHAKEN validation on incoming calls.	
Gap/Overlap	Tells agencies about gap or overlap discovered by ECRF/LVF in GIS data	
ECRF handles any standard shape	Location can be specified by polygon, circle, ellipse, or arc band, in addition to point	
ECRF returns service boundary	ECRF can return a polygon, within which, the response will still be valid	
ECRF Supports lost-planned-changes	allows planned changes in GIS to occur on a schedule	
matchType and degradedMatch implemented	Allows querier to know how validation was determined and receive a warning that validation was not necessarily as good as intended	
i3v3 Appendix B/NG GIS implemented	Updated GIS provisioning data model	
Support CLDXF location	US profile of PIDF-LO, FGDC conformant.	
Internal and External ECRF/LVF supplied	ECRF and LVF (Location Validation Function) for public and OSP support available on the Internet, separate from internal ECRF/LVF available on ESInet	
ECRF/LVF replica support	Interface that allows an OSP or other entity to maintain a local copy of the ECRF/LVF	
Interconnected ESInet support	Allows neighboring ESInets to connect to the State ESInet. Supports bidirectional ECRF/LVF query, call transfer, etc.	
Forest Guide Support	Entry in FG for State ECRF/LVF, and recursive resolution of out of area queries via the FG	

v3 Standard Requirements	What Does It Do?	**Status in Proposed Solution?** (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
MCS (MSAG Conversion Service) and GCS (Geocode Conversion Service) are implemented	MCS = MSAG (Master Street Address Guide) Conversion Service, converts between MSAG form of address and PIDF-LO. GCS=Geocode conversion service, provides civic to geo, or geo to civic conversion for any system	
Change in GIS results in routing change in minutes	A change in the GIS data can affect routing within minutes of the GIS authority releasing the change	
MDS implemented	Map Database Service returns maps (as images) or features to support both local and out of area maps	
Spatial Interface is implemented	Standard was to provision ECRF/LVF/MDS/GCS/MCS	
Changes to PRR effective on next call	Update of PRR policy in Policy Store causes changes in routing immediately	
i3v3 DR interface and all defined DRs implemented	Automated Discrepancy Reporting mechanism and several standard DR formats	
i3v3 Test call is supported	Automated mechanism to test the call path. No human required. Includes media check (loopback)	
i3v3 Test Call Generator supported	Automated mechanism to generate test calls (can text PRR sets)	
IS-ADR search supported at PSAP	Standardized way to check outside sources to see if they have additional data for a telephone number (like RapidSOS)	
humintlang tag supported	Signals request for language used on a call	
Call Transfer follows i3v3 call flows	Either Ad hoc or Route All Calls Via a Conference Aware UA (User Agent) model is followed for bridge based attended transfer	
Transfers between ESInets with different bridge models supported	Transfer of calls between ESInets that have different bridge models work as defined in the i3V3 standard	
Media server supports i3v2 IMR	Standardized multimedia "Interactive Voice Response" unit (auto answer with menus). Includes audio, video, text, RTT. Includes VXML for control.	

v3 Standard Requirements	What Does It Do?	**Status in Proposed Solution?** (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Logging service supports all i3v3 LogEvents	Logging Service supports all i3 defined log events	
NGCS elements create the specified LogEvents	All NGCS elements generate all V3 standardized log events they should implement	
Logger logs media per the standard	Logging service logs all media per the standard	
Logger retrieval interface follows standard	Logging Service implements i3 standardized log retrieval interface	
Logger can be used as IRR (Instant Recall Recorder)	Logging Service implements the Instant Recall Recorder function	
LNG supports P-Preferred-Identity + ESN/IMEI for non-initialized mobile	LNG retrieves IMEI for non-initialized phones and passes it in SIP P-Preferred Identify header	
Outgoing Call Interface Function	Supports call backs and other outgoing calls with all media supported on the incoming emergency call. Includes support for STIR/SHAKEN signing of Identity.	

Remainder of page intentionally blank

C. WORK PLAN AND PROJECT PLANNING

This section defines the required plans, methods, staffing, testing, and governance for implementing, accepting, and operating the NG911 solution. In this section and throughout this document (and as noted in the Glossary), ***'Respondent'*** refers to the proposing entity pre-award, and ***'Contractor'*** refers to the awarded entity post-negotiation and post-award. Any references to ***'Vendor'*** identify any third party from whom the Respondent or Contractor (as applicable) procures goods or services to fulfill the requirements of this RFP and subsequent contract, including hardware, software, connectivity services, and external personnel.

1. Project Management

a. Project Management Approach

The Respondent shall describe a project management approach aligned with Project Management Institute (**PMI**) best practices and informed by the Information Technology Infrastructure Library (**ITIL**) for service transition and operations. The approach must cover governance, control of scope, schedule, and budget, risk and issue management, stakeholder communications, and status reporting. Post-award, the Contractor shall execute this approach.

b. Project Manager

The Respondent shall assign a dedicated **Project Manager (PM)** as the single point of contact. The PM is responsible for scope, schedule, budget, resources, risks, and stakeholder communications; must hold the Project Management Professional® (**PMP)** certification; and have **≥5 years**' experience leading projects of comparable size and complexity, preferably in public safety or telecommunications.

c. Preliminary Plan (Project Management Plan [PMP])

The Contractor shall develop and maintain a living PMP consistent with PMI. The PMP will be used to monitor and control installation and deployment and must be kept current with State visibility and approval of changes via the Change Management process.

Minimum PMP contents:

- **Work Breakdown Structure (WBS), scope, deliverables, and schedule** (with milestones and the explicit handoff from implementation to service management).
- **Quality Assurance and Quality Control (QA/QC)** processes and acceptance criteria.
- **Risk and issue management** (registers, mitigation strategies).
- **Change Management Plan** and **Configuration Management Plan**.
- **Communications and Status Reporting Plan** (cadence, formats, dashboards, programmatic notifications).
- **Deployment and transition plan and schedule**, including a PSAP-by-PSAP work plan.

Notes:

- The PMP will be referenced regularly during implementation to ensure timely completion. -

- Any schedule or work-plan changes require prior State approval through the Change Management process. -

2. Staffing and Qualifications

a. Key Personnel

Identify **Key Personnel** (e.g., Project Manager, Technical Lead, Security Lead, Service Manager, Technical Engineer/Coordinator, Provisioning Coordinator). Provide resumes showing experience, qualifications, and relevant certifications. The State reserves approval rights for all Key Personnel and subsequent changes. Provide **30 days' written notice** before a Key Person's departure.

b. Staff Qualifications

The contractor shall supply qualified, experienced personnel devoted to successful contract performance and, upon State request, remove or replace Key Personnel.

c. Designations, Certifications, and Licenses

Provide evidence that assigned personnel – especially Key Personnel – hold the professional designations, certifications, and licenses necessary to perform their roles effectively.

3. **Implementation**

   a. **Implementation Approach**

   The Respondent shall describe an end-to-end approach for implementing **ESInet** and **NGCS** to deliver NG911 to all PSAPs. The State will assist with coordination and scheduling; the Contractor is responsible for planning and executing all activities. No service, system, or function is **Accepted** until the State provides written approval after successful testing and cutover readiness.

   b. **Elements of Implementation**

   Provide a comprehensive implementation plan that addresses the full project lifecycle – from design and engineering through testing, training, and final system cutover – aligned with NENA Standards and industry best practices.

   At a minimum, the implementation plan should address:

   - Methodology for implementing the entire NG911 system, establishing call delivery from all OSPs to all PSAPs across the State of Nebraska
   - Methodology for administering and operating the NG911 system for the contract term.
   - IP routing plan, how requirements are met, and governance of routing changes and documentation.
   - How NGCS will operate with the ESInet, and how each Functional Element will deliver required functionality.

4. **Transition**

   a. **Transition Plan: Current and Future**

   This procurement may require transition from existing systems and/or services provided by the current service provider. The Respondent shall provide a **Transition Plan** ensuring services are not **diminished, interrupted, or disabled** and that **SLA metrics remain enforced** during transition.

   Minimum topics:

   - Transition schedule with milestone dates for design, development, testing, implementation, and cutover to full operational readiness.
   - System testing approach during transition.
   - PSAP/site cutover approach, including **phased migration** and **parallel operation** with current systems.
   - **Contingency and rollback plan** for implementation or integration failures.
   - Risks, dependencies, and interdependencies affecting cutover.
   - **OSP interface** transition and service migration to the NG911 system.
   - Integration with other systems, services, and providers.

   Responsibilities: If a new provider is selected, the Contractor must engage the current provider and coordinate the transition. If a transition **away** from the Contractor's system is required later (including contract expiration), the Contractor shall cooperatively plan and execute the transition. Current 911 call delivery, features, functions, capabilities, and operations **must not be limited or impacted** by the proposed solution.

5. **Testing and Acceptance**

   a. **Testing (Comprehensive Test Plan)**

   System testing is required **before acceptance** of any component or function **and before cutover** to full operational status and commencement of payment. With the proposal, provide an **example NG911 System Test Plan** covering each element of the proposed system. Post-award, the test plan must be submitted to the State for approval at least thirty (30) days prior to the start of testing of any system function or components.

   The comprehensive test plan will address, at minimum:

   - Test environment, facilities, and equipment.
   - Test configurations and thresholds.
   - Simulators and test-call processes.
   - Final documentation of all tests and results.

   System Testing must address, at minimum:

   - NENA-STA-010.3 Functional Element testing.

- 911 call flow: primary, alternate, last route.
- End-to-end traffic flow.
- Functional Element ↔ Functional Element tests.
- Protocol ↔ Protocol tests.
- Port ↔ Port tests.
- Load testing: unexpected surge, short burst, sustained overflow.
- ESInet throughput and capacity.
- ESInet end-to-end connectivity (fault tolerance, failover, alternate routing, monitoring systems, fault notification).
- Security controls: firewalls, intrusion detection systems, intrusion prevention systems.
- Throughput acceptance testing of ≥24 hours, simulating 200% peak traffic load.

State participation and rights: Share results with the project team prior to acceptance; the State may require re-tests and may assign observers. The State may inspect test equipment and/or applications and must approve remediation actions from failed tests.

b. Test Plan Methodology

Describe the methodology for testing **all** NG911 system components, including those provided by Subcontractors or other suppliers, addressing the coverage area in §C-5.a. (Testing). Include **regression testing** procedures following defect remediation.

c. System Acceptance Testing

Acceptance testing must be completed prior to the State's final acceptance of the system. Final certification and system acceptance occurs **only after** the Contractor has provided acceptance test results to the State **and** the State has certified that the testing satisfactorily meets all requirements.

The Respondent must describe their approach for documenting the test results and may use the following codes to discuss their methodology:

- TP – Test Passed
- TF – Test Failed
- RTP – Retest Passed
- RTF – Retest Failed
- NA – Feature not applicable to the final configuration

On any failure the Contractor shall correct the deficit and perform regression testing to re-validate and re-certify all affected tests. Results of failed tests shall be documented and presented in writing to the State. Successful regression testing results must be delivered to the State

d. Independent Validation and Verification (IV&V)

Upon acceptance, the State will conduct IV&V testing using a third party. The Contractor shall collaborate to establish IV&V scope and priorities and support execution.

The Respondent MUST state acceptance of third-party IV&V testing of all elements required in this procurement document in its response to this RFP.

Remainder of page intentionally blank

D. DELIVERABLES AND DELIVERABLE APPROVAL PROCESS

The PSC and the State recognize that the **Contractor is responsible for end-to-end traffic from caller to call-taker**. This includes the **OSP ingress to the point(s) of interconnection (POI)** and the **delivery from the ESInet to the PSAP's call handling equipment (CHE)**.

The Contractor is responsible for all requirements in this RFP, including providing a **comprehensive risk assessment** of administrative, operational, and technical factors that could prevent achievement of the **99.999% availability** service level for the end-to-end system. The assessment must identify, at a minimum, areas with limited physical diversity, underestimated redundancy, or single-threaded network resources, and propose mitigation for each.

1. ESInet Architecture and Design

System Requirements:
Deliver a managed IP-based ESInet conforming to NENA i3 architecture, supporting legacy PSTN and SIP call flow, IPv4/IPv6 addressing, QoS mechanisms (e.g., DiffServ), and traffic segregation. Ensure no single point of failure through diverse network paths for the entire system, redundant nodes and functional elements, redundant data centers, and automatic failover (RPO <1 minute, RTO <5 seconds). Provide scalable bandwidth with traffic shaping and congestion management.

Deliverables:

- Detailed network architecture diagrams including IP addressing, VLANs, QoS policies, diversity topology, and redundancy model.
- Demonstration of SIP TLS and SRTP call signaling, media traversal with zero packet loss during failover.
- Documented RTO RPO targets, MTTR SLAs (<2 hours for critical issues), and failure mode analysis reports.

2. NG911 Core Services (NGCS)

System Requirements:
Supply or interoperate with NGCS components (BCF, LVF, LIS, ECRF, ESRP, PRF, LNG) per NENA standards, supporting SIP interfaces to all interconnections, PIDF-LO, and HELD protocols. Ensure performance (e.g., 200 millisecond median lookup latency, 10 queries per second), scalability for peak loads, and isolation capabilities. Log all transactions with timestamps, correlation IDs, and searchable storage.

Deliverables:

- Provide a mapping / traceability document aligning proposed system and service modules to NGCS functions and interface conformance statements.
- Interoperability test results with SIP calls and packet traces.
- Performance test results and scalability benchmarks.

3. GIS and Location-Based Routing

System Requirements:
Implement NENA-compliant GIS data model NENA-STA-006.2-2022 for ECRF/LVF, supporting civic/geodetic location validation and routing. Use PIDF-LO for location transport, enable push pull delivery to PSAPs, and support Policy-based routing (with PRF) with alternate routing logic. Provide GIS data versioning, automated updates, and provisioning APIs.

Deliverables:

- GIS data model documentation, sample datasets, and entity-relationship diagrams.
- Demonstration of location-based routing to the correct PSAP mapping for civic geodetic inputs, including edge cases.
- GIS update procedures and API specifications.

4. **Security, Privacy, and Trust**

System Requirements:
Implement NENA NG-SEC model with mutual TLS, RBAC, MFA, and encryption (TLS 1.3, AES-256). Mitigate DDoS/TDoS/SIP attacks via rate limiting and anomaly detection and blocking, isolation when necessary. Manage certificates, and provide incident response plans, vulnerability management, and SIEM integration.

Deliverables:

- Security architecture diagrams, PKI policies, RBAC matrices, and access control configurations.
- Recent penetration test reports and SLAs for patching.
- Demonstration of mutual TLS, anomaly detection, and SIEM log integration.

5. **Logging, Reporting, and Call Detail Records**

System Requirements:
Log all ESInet NGCS events with timestamps, correlation IDs, and tamper-evident mechanisms. Generate NENA compliant CDRs capturing call details to deliver to the Statewide reporting system. Retain logs' CDRs for a defined period of time (which may be different for each jurisdiction) with secure, searchable storage.

Deliverables:

- Sample logs, CDR schemas, retention procedures, and RBAC policies.
- Demonstration of CDR generation, search/export, and operational reports.
- Evidence of tamper-evident storage and audit trails for admin changes.

6. **Interoperability, Testing, Conformance, and System Acceptance**

System Requirements:
Demonstrate NENA i3 conformance via self-attestation and multi-vendor interoperability tests. Conduct phased testing (unit, integration, failover, performance at 150% capacity, security) with 100% pass rates for critical flows. Provide comprehensive documentation and training.

Deliverables:

- Test plans, conformance matrices, and interoperability test schedules.
- Pilot lab demonstration with KPIs (e.g., 99.999% uptime).
- User manuals, API specs, and training curricula.

7. **Operational Support and Service Level Agreements (SLAs)**

System Requirements:
Commit to SLAs (99.999% availability, <2-hour MTTR for Priority 1 issues, 15-minute acknowledgment). Provide training, runbooks, and documentation using NENA terminology. Implement change management with maintenance windows, rollback procedures, and 30-day notifications.

Deliverables:

- SLA documents, training curricula, sample runbooks, and maintenance calendar.
- References from three comparable NG911 deployments with uptime reports.
- System and Service provided must be delivered compliant with NENA standards at acceptance unless mutually agreed upon provisions are acceptable. In this event, the contractor must provide a plan, timeline and communicate regularly with the State and the Advisory Committee on progress to full NENA standard conformance.
- Furthermore, as Standards evolve the contractor ***MUST MAINTAIN*** conformance with any new revisions to standards listed as requirements in this RFP. The State will allow a period of 9 months for the contractor to

become compliant as a guideline. It is incumbent on the contractor to identify any areas they may be unable to meet the 9-month target and produce a plan and timeline to achieve conformance.

Submission Requirements

- Respondents must provide a written reply for each requirement within this RFP with descriptions of their proposed system (unless otherwise noted) and services to meet or exceed the requirement. If a requirement is not fully met, an exception can be made but any exception must include an alternative. If a requirement is on a roadmap for future implementation that must be clearly identified with a timeline that shows when deployment is expected.
- Provide a detailed project plan, including timelines, milestones, and resources for deployment, testing, and ongoing support.
- Submit all deliverables in electronic format, including architecture diagrams, test reports, sample logs, and documentation.

Deliverables are subject to the Deliverable Approval Process, contained in the terms and conditions.

Remainder of page intentionally blank

E. TECHNICAL REQUIREMENTS

1. ESInet Requirements

The Emergency Services IP Network (ESInet) must comply with NENA-STA-010.3-2021 (i3 Standard) and follow the recommendations in the NENA Emergency Services IP Network Design (ESIND) Information Document (NENA-INF-016.2-2018). The ESInet shall interconnect all NG911 components with Public Safety Answering Points (PSAPs) and Originating Service Providers (OSPs) using Internet Protocol (IP), and, where necessary, legacy methods.

The Respondent shall provide an ESInet design that conforms to the NENA i3 architecture for a managed IP-based emergency services network. The design shall support multi-tenant interconnects with the Public Switched Telephone Network (PSTN) and Session Initiation Protocol (SIP), diverse physical routing paths, and network-level redundancy that eliminates any single point of failure. The ESInet must natively support IPv4 and IPv6, implement Quality of Service (QoS) to prioritize emergency traffic, and use virtual routing or equivalent technologies to segregate emergency services traffic from non-emergency traffic. The design shall include scalable bandwidth to handle peak loads, with automatic traffic shaping and congestion management.

The ESInet shall support SIP per **RFC 3261** and applicable NG911 SIP extensions, including SIP over **Transport Layer Security (TLS)** for signaling and **Secure Real-time Transport Protocol (SRTP)** for media. Standard transports, including full IPv6 compatibility shall be supported, including TLS over TCP, and UDP where applicable. Interfaces must support both location-by-reference and location-by-value conveyance to ensure seamless integration with OSPs.

The ESInet shall support standard cross-connect and peering arrangements, selective routing, and boundary elements such as **Border Control Functions (BCFs)**. **Border Gateway Protocol (BGP)** shall be used for multi-site reachability and load distribution. The Respondent shall provide documented procedures, application programming interfaces (APIs), and configuration templates for peering with adjacent ESInets, third-party providers, and legacy networks, including policy-based routing and traffic-exchange agreements.

The ESInet shall incorporate geographically diverse, redundant network cores; duplicate session border/edge elements; and automatic, transparent failover for signaling and media so that failure of any single component (e.g., link, router, or server) does not disrupt 911 service. The Respondent shall define and guarantee a **Recovery Point Objective (RPO)** of less than one (1) minute and a **Recovery Time Objective (RTO)** of less than five (5) seconds for critical paths, with active-active or active-passive configurations across data centers separated by at least 100 miles.

The ESInet shall enforce Differentiated Services (DiffServ) or equivalent QoS policies to prioritize 911 signaling (for example, SIP INVITE transactions) and media streams, with configurable DSCP markings. It must support bandwidth provisioning, traffic policing, and shaping to maintain PSAP-grade voice quality (Mean Opinion Score [MOS] greater than 4.0) and data integrity under load, including mechanisms to handle burst traffic and to prevent overload.

The Respondent shall supply a comprehensive **Network Management System (NMS)** or **Element Management System (EMS)** with real-time dashboards; syslog export; SNMPv3 polling and traps; and key performance indicators (KPIs) including latency, packet loss, jitter, and utilization, aligned with NENA operational guidance. The system must provide threshold-based alerting, historical trend analysis, and integration with external tools via APIs.

The Respondent must provide a description and/or documentation that supports the requirements in this section, including a clear description of:

- Network operations management (operational policies, staffing, incident response, and system management procedures).
- Detailed physical and logical security measures (encryption protocols, access controls, secure access points, and physical security for data centers); strategies for achieving 99.999% uptime with contingency plans.
- Continuous performance monitoring mechanisms with logging and alert systems; real-time alarm generation and notification strategies.
- Guidelines for routine, updates, and emergency maintenance; comprehensive disaster recovery plan with RTO and RPO details.
- Procedures for service restoration post-incident.
- Proactive outage prevention and response strategies including redundancy testing.

- Technical specifications for core routing architecture with diverse paths and load balancing.
- Interfaces with hosted solutions or third-party providers.
- Fault zone design methodology identifying critical components and failure points.
- Bandwidth management protocols prioritizing emergency traffic.
- And any bandwidth sharing arrangements with implications for priority traffic.
- Any limitations in the "span of control" over connections to the OSPs or PSAPs that are linked to the ESInet to establish a risk register for future reference.

Additionally, the Respondent must investigate and document potential single points of failure, explain detection and activation of standby systems if not active-active, and detail ESInet interconnection points with OSPs and PSAPs for full IP-based NG911 functionality.

1.1. Architecture and Topology

1.1.1. ESInet Diagrams

The contractor must submit comprehensive diagrams that visually represent the proposed ESInet architecture. **These diagrams must be kept current and be included in a configuration management database that the 911 Advisory Committee and the State may access at any time during the contract to validate the deployment and system functionality.**

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Comprehensive diagrams illustrating network maps (logical and physical topologies).
- Physical and logical path diversity for redundancy.
- One-time and transitional network elements.
- Network ingress and egress points with connections to OSPs, PSAPs, and external interfaces.
- Transport types (e.g., MPLS or Ethernet) with port speeds.
- Capacities and estimated bandwidth at ingress, core, and egress points.
- Interconnection locations (nodes, data centers, POIs, LRGs); and any additional technologies and interfaces.

1.1.2. ESInet Interconnection

The ESInet must facilitate seamless interconnections with neighboring states or regions upon deployment. The ESInet shall use the **Border Gateway Protocol (BGP)** as the sole **Exterior Gateway Protocol (EGP)**.

Newly established ESInets in cooperating states must be able to connect to the State ESInet within a designated timeframe. To ensure robustness and resilience:

- Interconnection should occur at a minimum of two mutually agreed-upon points to guarantee redundancy.
- Bandwidth provisioning must cater to **at least 200% of anticipated peak call volume**, ensuring ample capacity and robustness.
- Interconnecting methods and locations should be balanced equitably to manage costs effectively among partners.
- If neighboring ESInets do not adhere to the State's Differentiated Services Code Point (DSCP) specifications, the state's routers will remap DSCPs as deemed appropriate.
- The establishment of BGP between the State ESInet and neighboring networks is recommended.

All additional networks integrated with the ESInet must meet the specified minimum qualifications for interconnection to uphold security and performance standards. The State's security must be collaboratively protected by all involved network providers.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Seamless interconnections with neighboring states/regions upon deployment.
- Connection capability for new ESInets within designated timeframe.
- Minimum two interconnection points for redundancy.

- Bandwidth provisioning for 200% of peak call volume.
- Equitable interconnecting methods/locations for cost management.
- DSCP remapping if neighboring ESInets differ.
- Recommendation for BGP between networks.
- Minimum qualifications for additional integrated networks; and collaborative security protection by providers.

1.2. External and PSAP Connectivity

1.2.1. Originating Service Provider (OSP) Connection

Contractors are responsible for facilitating all necessary connectivity to allow traffic to flow from OSPs into the ESInet.

- Upon acceptance, sufficient bandwidth must be provisioned to support OSP traffic irrespective of connection method (CAMA, SS7, IP, etc.).
- Points of Interconnection (POI) must be deployed with the greatest extent of diversity possible. This means that the contractor ***shall be required*** to identify any situations where OSPs lack diverse connections to the POI(s).
- Where diversity is limited from an OSP to the POI, and/or from the egress gateway to the PSAP, or restricted for any reason, **the contractor must identify this as a risk to their NG911 service and discuss options with the PSC for limiting or eliminating the exposure of an OSP or PSAP if a lack of diversity may cause a disruption**.
- Careful design should ensure **redundancy and diversity from the caller to the call-taker** to ensure that the system is as diverse and redundant as possible from end-to-end.
- Communications must enable smooth migration to the ESInet once operational, including aggregation of legacy 911 traffic into the core network.
- Contractors must continuously monitor the bandwidth at aggregation points to efficiently manage and increase bandwidth as required.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Facilitation of diverse and redundant connectivity for OSP traffic flow into the ESInet.
- Provisioning of sufficient bandwidth for OSP traffic (CAMA, SS7, IP, etc.) upon acceptance.
- Smooth migration to ESInet with aggregation of legacy traffic.
- Redundant and diverse design for disruptions, interfacing with network gateways based on OSP capabilities.
- Identification of any risks to their system due to lack of diversity or redundancy from caller to call-taker.
- Identification of risks from limited diversity and options to mitigate exposure for OSPs or PSAPs.
- Continuous monitoring/increase of bandwidth at aggregation points.

1.2.2. PSAP Connection

At the point of system acceptance, the ESInet must guarantee sufficient bandwidth to support:

- **2 Mbps per PSAP + 2 Mbps per position** during standard operational conditions.
- **1 Mbps per PSAP + 1 Mbps per position** under conditions where network disruptions occur, which may include simultaneous failures of the largest link or comprehensive outages affecting all networks of a single ISP.

The contractor must commit to ongoing bandwidth monitoring throughout the contract duration and promptly increase capacity as necessary, including an annual growth factor of 10%.

The design must also facilitate interconnections with PSAP systems (like CAD and logging recorders), as well as with criminal justice networks and other secure public safety technologies, ensuring uninterrupted SIP traffic flow for 911 calls.

The ESInet shall allow for all egress connectivity, including gateways, and be configured to establish the capability for traffic to flow from the ESInet into the PSAP.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Guaranteed bandwidth of 2 Mbps per PSAP + 2 Mbps per position under standard conditions and 1 Mbps per PSAP/position under disruptions (e.g., largest link failure or ISP outage).
- Commitment to ongoing bandwidth monitoring and increases with 10% annual growth factor.
- Facilitation of interconnections with PSAP systems (CAD, logging recorders), criminal justice networks, and secure public safety technologies.
- Ensuring uninterrupted SIP traffic for 911 calls.

1.3. Legacy Interoperability

1.3.1. Legacy Network Gateway (LNG)

The Respondent must provide a Legacy Network Gateway (LNG) solution to serve as the ingress point for calls originating from legacy networks (e.g., wireline, wireless, VoIP) that have not yet transitioned to native i3 SIP origination. The LNG is responsible for converting legacy signaling to i3-compliant SIP and querying legacy ALI databases to obtain location information.

LNGs and/or LSRGs must conform to NENA-STA-010.3 and provide termination for all existing legacy OSPs until they migrate to i3 origination. The current solution utilizes an LSRG combining LNG and LSRG functions.

- Interface Compatibility:
  - The LNG must maintain interface compatibility with existing Selective Routers, allowing for minimal disruption and cost implications.
- Geographical Redundancy:
  - Legacy OSPs must have access to connections at two geographically diverse LNGs to enhance resilience.
- Legacy Support:
  - The LNG must be configured to manage legacy PSALI records, including migration processes outlined in the documentation provided.

LNG Connectivity to ESInet
The LNG must securely connect to the ESInet, receive calls from legacy network trunks (e.g., CAMA, MF), and interface with the ESInet's Border Control Function (BCF) to forward calls into the NG911 core.

Protocol Conversion (Legacy to SIP)
The LNG must convert legacy in-band signaling (e.g., CAMA wink-start, MF tones) and associated trunk supervision into i3-compliant SIP (RFC 3261) for processing by the ESInet.

ALI Query and Location Formatting
The LNG must use the Automatic Number Identification (ANI) received from the legacy call to perform a query against the appropriate legacy ALI database. It MUST then format the retrieved ALI data into a NENA-compliant Presence Information Data Format - Location Object (PIDF-LO) for inclusion in the outbound SIP INVITE.

Security, Logging, Monitoring, and Redundancy
The LNG, as a critical ESInet functional element, must adhere to the same stringent requirements for security, logging, monitoring, and redundancy as other core components to ensure system integrity and high availability.

If separate LNGs are proposed, they must:

- Maintain interfaces similar to current systems
- Support TTY to RTT conversion
- Provide E2 connections to all MLCs, GMLCs, and VPCs
- Be positioned outside the ESInet, before the BCF
- Support ElementState and ServiceState functionality

Each component has specific requirements for capacity, performance, integration, and conformance with NENA standards.

The solution must maintain appropriate spare parts at various locations to ensure immediate system restoration when needed, with specific requirements for inventory management, replacement schedules, and on-site spares at data centers.

The LNG must support the Service Order Activation (SOA) interface towards the legacy OSP, store data in the Location Database in LVF-valid form and convert to and from the legacy data format using the MCS.

The LNG shall support:

- Error checking
- GIS-based MSAG (for legacy OSP use)
- The Service Order Activation (SOA) interface towards the legacy OSP, store data in the Location Database in LVF-valid form and convert to and from the legacy data format using the MCS
- Service Order Address Validation
- Service Order Error checking
- Service Order history available/viewable for every telephone number
- Coordination with Telecommunications providers:
    - OSPs will be able to manage/make updates to their records directly in the database without having to submit SOI
    - OSPs will be able to run performance/statistical reports on their No Record Found (NRF)/Discrepancy and SOI processing
    - OSPs will be able to view discrepancies and NRFs directly from the web interface real time
- Data import / export
- Data integrity and availability
- ALI updates
    - OSP's have the ability to manually update their own records
    - OSP's have the ability to lock and unlock their own records
    - All manual updates be tracked in history
- Customer access to data
- Telco access to data
- Bulk modifications
- PSALI functionality
- Database reports
- NRF process
    - ALI discrepancies
- Tracking, reporting and timestamp for discrepancies and NRFs.
- Service Order exceptions
- ALI database audit
- MSAG database audit

The State expects the LNG to maintain connections to Text Control Centers (TCCs) so that NG PSAPs maintain a complete standard (NENA-STA-010.3) connection for Short Message Service (SMS) calls to 911 from legacy OSPs via the LNG.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LNG conformance to NENA-STA-010.3 for legacy OSPs until i3 migration.
- Interface compatibility with existing Selective Routers.
- Geographically diverse connections for legacy OSPs.
- Management of legacy PSALI records with migration processes.
- TTY to RTT conversion.
- E2 connections to MLCs/GMLCs/VPCs.

- Positioning outside ESInet before BCF.
- ElementState/ServiceState support.

1.3.2. Legacy Selective Router Gateway (LSRG)

A Legacy Selective Router Gateway (LSRG) must serve as the interface for legacy selective routers to terminate ISUP SS7 trunks utilizing an inter-tandem trunk group method of termination.

The LSRG must convert the call signaling to SIP/RTP, query the existing ALI data management system to retrieve location information for the call and then route the call to the next nominal "hop" based on a LoST query to an ECRF.

Additionally, the LSRG must be able to facilitate bi-directional communications with the legacy selective routers for both voice and data (star codes) transactions.

If Respondents utilize an LSRG for their proposed solution, they must include a timeline and plan for removing the LSRG during the contract period. The LSRG is to be only a temporary solution that can be used to initially gateway OSP traffic.

Any LSRG implemented as part of the Contractor's solution must conform to the NENA Legacy Selective Router Gateway (LSRG) Standard (NENA-STA-034.1-2022), and should be deployed to align with the relevant sections of the NENA NG9-1-1 Transition Plan Considerations Information Document (NENA-INF-008.2-2013).

LSRG Connectivity to ESInet and Legacy SR
The LSRG must provide a secure interface to the ESInet to receive routing queries from the ECRF and a separate, secure interface compatible with the legacy Selective Router's query/response protocol.

Routing Protocol Conversion (LoST to Legacy)
The core function of the LSRG is to receive a standards-based Location-to-Service Translation (LoST) protocol query (RFC 5222) from the ECRF, translate it into a format the legacy SR can process (often a proprietary format or a simplified query containing an ESN), and translate the SR's response back into a LoST response for the ECRF.

Security, Logging, Monitoring, and Redundancy
The LSRG must meet the same core requirements for security, logging, monitoring, and geo-diverse redundancy as other critical ESInet functional elements to ensure the integrity and availability of call routing.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Interface for legacy Selective Routers via ISUP SS7 trunks.
- Conversion to SIP/RTP.
- ALI query and LoST-based routing.
- Bi-directional communications for voice/data (star codes).
- Timeline/plan for LSRG removal as temporary solution for OSP traffic.
- Deployed LSRG (where applicable) in conformance with NENA LSRG Standard (STA-034.1)

1.3.3. Legacy PSAP Gateway (LPG)

The State requires **Legacy PSAP Gateways (LPGs)** that conform to NENA-STA-010.3. LPGs shall provide **origination for all legacy PSAPs until those PSAPs migrate to i3 termination**. **LPGs must allow PSAPs to continue to use existing equipment and processes except where NENA-STA-010.3 requires change** (for example, use of Pseudo-Automatic Number Identification [pANI]). Each LPG shall connect legacy PSAPs to the ESInet using SIP and legacy interfaces such as CAMA and ALI and shall convert NG911 SIP signaling and media to legacy protocols such as TDM and ISDN to maintain compatibility.

Protocol Conversion (SIP to Legacy)
The LPG must convert the SIP-based signaling and media from the ESInet into legacy circuit-switched formats (e.g., CAMA, ISDN PRI) that are compatible with the legacy PSAP's CHE.

Location and ALI Integration
The LPG must extract location information (PIDF-LO) from the incoming SIP signaling and convert it into a legacy Automatic Location Identification (ALI) format for delivery to the PSAP's ALI database/controller.

Text Support (TTY to RTT Conversion)
The LPG must support interworking between Real-time Text (RTT) on the ESInet, and legacy Baudot-based Teletypewriter (TTY) devices used in the PSAP, ensuring seamless communication for hearing-impaired users.

Call Transfer Support
The LPG must support call transfer scenarios, including the ability to relay transfer requests from the legacy PSAP back into the ESInet to enable transfers to other NG911-capable agencies or PSAPs.

Logging and Reporting
The LPG must generate detailed logs for all call processing events, alarms, and system activities and forward them to a central logging service in a standard format (e.g., Syslog) as defined by NENA standards.

Security Mechanisms
The LPG must implement robust security measures, including access control, authentication, and encryption, to protect the interface between the ESInet and the legacy PSAP network, adhering to NG911 security standards.

Monitoring and Maintenance
The LPG must be capable of being monitored for operational status, performance, and alarms. It must support standard monitoring protocols (e.g., SNMP) and provide mechanisms for remote administration and maintenance.

Geo-Diversity and Redundancy
The LPG must be deployed in a geographically diverse and redundant configuration to ensure high availability and failover capabilities, preventing a single point of failure from isolating a legacy PSAP.

Discrepancy Reporting
The LPG must support a mechanism for reporting discrepancies, such as call routing errors or ALI data problems, from the legacy PSAP environment back to the NG911 systems Discrepancy Report service.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- The LPG must be able to maintain the PSAP's existing ALI format.
- The LPG must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3.
- The State must be able to subscribe to ServiceState and receive the standard state change
- LPG connections shall allow for PSAPs to directly connect systems (cable IP) to the ESInet
- LPG queries ALI databases and maps NG911 location data to legacy formats.
- Converts TTY to RTT for text-to-911 in legacy PSAPs.
- Supports call transfers to/from legacy PSAPs, mapping i3 transfers to legacy systems.
- Logs call events, protocol conversions, and errors; supports discrepancy reporting.
- Implements TLS and authentication for secure connectivity.
- Monitors LPG performance; supports maintenance with minimal disruption.
- LPG deployed with geo-redundancy to ensure high availability.
- Reports errors in call delivery, location, or protocol conversion.

1.4. Network Behavior and Performance

1.4.1. ESInet IP Routing

The ESInet must follow the NENA standards to ensure that IP routing across the ESInet can handle all traffic effectively under varying conditions. **Ongoing bandwidth assessments, risk assessments, diversity, and redundancy testing must be documented and updated in a configuration management database as the ESInet evolves.** Proactive measures to trace IP routing within the diverse and redundant paths is required. Any change to the system must include testing of IP routing failover mechanisms prior to acceptance of a change.

No specific link shall be provisioned with **more than 50% of the physical limit** of that link to allow for expansion without physical changes to the link, router, or switch to which it connects. As changes in the network are completed, the IP address plan shall be updated and remain accessible to the State or designee.

- Every element proposed supports both IPv4 and IPv6 (dual stack).
- All elements in the network have globally routable IP IPv4 and IPv6 addresses.
- The network shall use one Interior Gateway Protocol (IGP) throughout, and no routers use Routing Information Protocol (RIP).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance with NENA standards for handling traffic under varying conditions.
- Documentation of ongoing bandwidth assessments, risk assessments, diversity and redundancy testing in a configuration management database.
- Proactive measures to trace IP routing in diverse and redundant paths.
- Testing of IP routing failover mechanisms prior to any system change acceptance.

1.4.2. ESInet Bandwidth

The ESInet is expected to deliver sufficient end-to-end bandwidth to accommodate traffic to and from PSAPs effectively.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Adequate sizing must consider 911 voice and video calls, text communications, data transmissions, and a calculated surge factor based upon the State of Nebraska PSAPs.
- An **annual growth factor of 10%** must be incorporated into capacity planning.
- Bandwidth sharing with other networks within the State of Nebraska is encouraged, **especially for secondary routes, provided the contractor implements provisions to ensure that using these networks does not impact the primary ESInet performance.**
- The ESInet should be structured for future expansion, allowing scalable growth throughout the duration of the contract without impeding current services. A detailed plan should outline how the ESInet will readily accommodate increases in bandwidth, as necessary.
- A detailed plan for scalable expansion throughout the contract without impeding services.

1.4.3. Quality of Service (QoS)

The ESInet must provide Quality of Service (QoS) features at all ingress, core, and egress points.

The ESInet must employ DiffServ throughout, adhering to packet marking specifications per NENA-STA-010.3. A commitment to maintaining packet loss below 0.5%, jitter under 15 milliseconds, and (one-way) latency below 25 milliseconds is required during standard operational periods.

- Performance metrics for these characteristics should be established on a standby measurement basis, with the State stakeholders allowed to initiate specific measurements as required.
- Regular reporting must provide comprehensive insights into network performance metrics, including averages and worst-case scenarios.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Employment of DiffServ throughout with packet marking per NENA-STA-010.3.
- Commitment to packet loss below 0.5%, jitter under 15 milliseconds, and one-way latency below 25 milliseconds during operations.
- Standby measurement basis for performance metrics with State-initiated measurements.
- Regular reporting on network performance including averages and worst-case scenarios.

1.4.4. Traffic Flow Requirements

Respondents must describe how traffic will flow from end to end across the network in a fashion that is compliant with applicable standards. ESInet and NG Core Services functions be described to allow the evaluator to clearly identify where specific operations on the traffic occur. If necessary, diagrams may be used to assist the visualization of traffic flow through the proposed solution.

The ESInet and NGCS must operate in concert with one another to establish the flow of traffic from the caller to the call-taker. This flow of traffic utilizes physical and logical connections to the resources required for call delivery. Traffic flow shall include a description of traffic flow under **NORMAL** operating conditions and traffic flow under **ABNORMAL** operating conditions.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- End-to-end traffic flow description compliant with standards.
- Identification of operations on traffic in ESInet and NGCS.
- Diagrams for visualization if necessary; traffic flow under normal and abnormal conditions.
- Handling of use cases such as legacy OSP to NG PSAP, NG OSP to NG PSAP, Internet to NG PSAP, text/ALI/GIS traffic, virtual PSAPs, BCF to ECRF, ECRF to SI/ESRP/PSAP/LPG, LSRG to OSP, OSP to LNG, logging/recording, and monitoring/management. Additional or modified use cases specific to the solution should be expanded upon.

1.4.5. Traffic Shaping

Respondents must include a description of where traffic shaping will be employed, detailing the techniques used and their intended benefits. A formal **traffic shaping policy document** must be created, ensuring transparency and regular updates are made available to State personnel.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Description of where traffic shaping is employed, the techniques used, and their intended benefits.
- Creation of a formal traffic shaping policy document with transparency, regular updates, and availability to State personnel.

1.4.6. ESInet Network Time

Network Time Protocol servers must be provided. The NTP servers must provide service to all elements in the ESInet including all PSAPs and other agencies on the ESInet. Time service must permit every system and every agency to maintain time within 1 millisecond of absolute time with 4 nines (99.99%) availability. The network shall have a hardware clock. However, in no circumstances, including failure of the hardware clock, must time as maintained by the time server(s) vary by more than 20 milliseconds from absolute time.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Provision of NTP servers serving all ESInet elements (NGCS FEs, PSAPs, agencies) within 1 millisecond of absolute time with 4 nines (99.99%) availability.
- Preference for hardware clock but ensuring no more than 20 millisecond variances even on failure.
- Descriptions of NTP service provision, confirmation of 1 millisecond accuracy with 4 nines availability, and meeting 20 millisecond variance threshold.

1.5. Resilience and Service Levels

1.5.1. ESInet Availability

The ESInet must maintain the integrity of ***emergency call processes, ensuring availability of 99.999% at all network points (Ingress, Core, Egress)***. Key provisions include:

- The entire call path must be resilient and monitored for compliance with the availability standard.
- Support services not related to call handling should achieve an availability of 99.9%.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Resilience and monitoring of the entire call path for 99.999% availability at ingress, core, and egress with clear identification of any boundaries that are outside of the span of control of the contractor which may be a risk to achieving five nines (e.g., OSP ingress, PSAP egress). 99.9% availability is acceptable for non-call-handling support services.
- Uptime calculations assessing physical device MTBF for critical equipment in serial/parallel configurations.
- A comprehensive sparing plan for all sites with replacement strategies.
- Established technician response times for outages.
- Calculated MTTR based on spares and response times.
- A consolidated overview of overall availability combining MTBF and MTTR data.

1.5.2. ESInet Reliability

The design of the ESInet must emphasize reliability through strategic diversity across geographic regions, technology, and vendors. Each node within the network must utilize **at least two routers from different manufacturers** to deliver redundancy. If this is unfeasible, a rationale for maintaining reliability under specific failure conditions must be provided. **No segment of the network should hinge on a single point of potential failure, such as a "backhoe incident."**

The reliability design must conform to guidelines specified in the FCC Report and Order 13-158 aimed at enhancing 911 reliability across all communication networks.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Strategic diversity across geographic regions, technology, and vendors.
- Use of at least two routers from different manufacturers per node for redundancy (or rationale if unfeasible).
- Elimination of single points of failure (e.g., "backhoe incident").
- Conformance to FCC Report and Order FCC 13-158 for enhancing 911 reliability.

1.6. Operations and Management

1.6.1. ESInet Monitoring and Management

A dedicated 24/7/365 Network Operations Center (NOC) must oversee continual ESInet monitoring to ensure immediate detection of any functional disruption within the system. §E-9.3.1 contains minimum NOC requirements that must be met as part of this proposal.

- **All network links require constant congestion monitoring,** with timely mitigation strategies implemented by contractors.
- **Failure alerts should be generated within a minute for any link or component malfunction** of the ESInet.

Thresholds for triggering mitigation must be explicitly delineated, especially in response to network congestion, with proactive communication to the State regarding the mitigation plan, implementation timelines, and ongoing progress reports.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A dedicated 24/7/365 NOC for continual monitoring and immediate detection of disruptions.
- Constant congestion monitoring of links with timely mitigation.
- Failure alerts within 1 minute for malfunctions.
- Explicit thresholds for mitigation (e.g., congestion).
- Proactive communication to the State on mitigation plans, timelines, and progress.

1.6.2. ESInet Maintenance Window

The proposed ESInet **must have no scheduled down time.** If maintenance is required, which would temporarily cause the network to have lower than 99.999% availability while the maintenance activity is underway, the contractor must provide a **pre-maintenance risk register** prior to commencing the maintenance and complete the maintenance under the terms of §E-9.5.1 (Change Management Requirements) and §E-9.5.2 (Scheduled Maintenance Process) below. **No maintenance activity which, if improperly completed, which could cause an outage of any part of the network, shall be permitted outside the terms of §E-9.5.1 and §E-9.5.2.**

All maintenance activity must be preceded by a Maintenance Operation Plan (MOP) required **at least 14 days** prior to the maintenance. The MOP shall include the provisional operating configuration to ensure that performance continually meets the 99.999% service level as the maintenance is being performed.

Scheduled downtime is unacceptable under routine operations. If maintenance is essential, it must follow as stringent Scheduled Maintenance Process to maintain or exceed 99.999% availability. Any maintenance that could jeopardize network functionality **must be strictly controlled.**

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- No scheduled downtime; completion of any maintenance impacting availability under specified terms (§E-9.5.1 and §E-9.5.2).
- Prohibition of maintenance causing outages outside those terms.
- Requirement for a Maintenance Operation Plan (MOP) at least 14 days prior, including provisional configurations to maintain 99.999% service level.
- Descriptions of handling no-downtime requirements, planning/conducting maintenance without impacting availability, and the MOP process for guiding activities.

1.7. Implementation Details

1.7.1. Port Mapping

Comprehensive documentation of port block/mapping/forwarding policies must be maintained, providing access to both the State and PSAPs. This documentation should include provisions that allow stakeholders to request traffic on specific ports to be allowed from external sources into predetermined network points.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Comprehensive documentation of port block/mapping/forwarding policies accessible to the State and PSAPs.
- Provisions allowing stakeholders to request traffic on specific ports from external sources to predetermined network points.

Remainder of page intentionally blank

2. Next Generation Core Services (NGCS) Requirements

The proposal must include a **Next Generation Core Services (NGCS)** implementation deployed across **multiple redundant data centers.** The system shall use **at least three (3) data centers,** with a preference for **at least one in-state** and at least **one geographically distant** (more than 100 miles away – preferably several states away) to avoid common-cause failures such as severe weather or localized incidents. The state will permit a shared facility but prefers a **separate NGCS instance** (distinct virtual machines and management) from other tenants. Each NGCS component – physical and virtual – must be **redundantly deployed in every data center** with **no single point of failure.**

The NGCS must also be **isolated and resilient** against external threats and against faults arising elsewhere in the provider's NG911 ecosystem. Respondents must **describe and demonstrate** how their design prevents impact from incidents in another ESInet or statewide NGCS service offered by the provider, ensuring Nebraska's NG911 operations continue **without degradation.**

All NGCS elements which use policies must retrieve policies from a NENA-STA-010.3-compliant policy server and must be **provisioned with the host name of the policy server it uses.** See §E-2.2.1.1 for the NGCS Policy Store requirements.

- The State desires redundant functional elements, including **all databases to be deployed active-active such that all redundant elements are actually serving traffic at all times.**
- The Respondent must state which functional elements and databases are not actually serving traffic at all times and for each such element; the mechanism for failover that will reliably guarantee the **99.999% availability requirement of the entire system.**
    - **For active-active elements**, the Respondent must describe how the client determines an element has failed, and how it recovers (typically via retry), noting what the worst-case timing for the detection and retry is, and how the appropriate Service Level Objective within that Service Level Agreement is maintained.
    - **For each database**, and **each call-state data object**, the Respondent must describe how state is reliably maintained, and failover within the 99.999% availability is assured, including any retry operations required at the client.
    - **For databases that are updated at call time**, the Respondent must describe the replication strategy, specify a maximum data sync time, and describe how it is achieved. Note that the State requires the ability to update a service boundary polygon in the ECRF dynamically, and replication/data sync of that operation must be described in the proposal.
    - The State expects that the LPG, LNG, and MCS be the only element that supports legacy functions.

The contractor shall **supply or ensure interoperability with all NGCS functional elements as defined by NENA,** including but not limited to the Location Validation Function (LVF), Location Information Server (LIS), Emergency Call Routing Function (ECRF), Emergency Services Routing Proxy (ESRP), Policy Routing Function (PRF), and Legacy Network Gateway (LNG). All elements must expose the NGCS interfaces specified in the standard, with the contractor documenting implementation details for each (e.g., integrated software modules, hosted cloud services, or third-party integrations). The system must support bridging to legacy systems via appropriate gateways.

All NGCS interfaces shall adhere to defined specifications, including SIP messaging extensions, RESTful APIs (using JSON/XML payloads), and NENA-defined ESInet ↔ Core interfaces. Payloads and schemas must comply with NENA requirements, such as Presence Information Data Format – Location Object (PIDF-LO) for location data, with support for HTTP-Enabled Location Delivery (HELD) protocols.

NGCS components (e.g., ECRF queries, LVF validations) **must achieve performance targets**, including lookup latency SLAs of 200 millisecond median and 500 milliseconds at the 95th percentile under peak load (jurisdiction may adjust based on scale). The system must handle at least 10 queries per second per component with no degradation.

The NGCS must scale horizontally to support jurisdiction-specific peak call rates (e.g., 1,000 calls per hour per PSAP) and data volumes, with tenant isolation for multiple PSAPs via virtual instances or containers. It shall enable dynamic provisioning of PSAP service boundaries through administrative interfaces.

All NGCS transactions shall be logged comprehensively, including timestamps, full request/response payloads (redacted for privacy where necessary), originator identities, correlation IDs, and error codes, enabling end-to-end tracing across components. Logs must be stored in a searchable database with retention support.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NGCS deployment in multiple redundant data centers (preference for at least 3, with one in-state and one >100 miles away).
- Preference for separate instances (different VMs) if sharing data centers.
- Redundant deployment of all components without single points of failure; resistance to external threats and internal disruptions from other ESInets/NGCS.
- Description/demonstration of unimpeded operation during disruptions.
- Policy retrieval from NENA-STA-010.3-compliant policy server with host name provisioning.
- Preference for active-active redundant elements/databases serving traffic at all times.
- Statements on non-active elements with failover mechanisms guaranteeing 99.999% availability.
- Descriptions of failure detection/recovery for active-active elements (worst-case timing, SLO maintenance).
- State maintenance/failover for databases/call-state data.
- Replication strategy for call-time updated databases with max sync time.
- Dynamic ECRF service boundary updates with replication/sync description.

2.1. Edge Security and Ingress

2.1.1. Border Control Function (BCF)

The BCF must conform to NENA-STA-010.3 standards, preferably constructed from a commercial Session Border Controller (SBC), Firewall, and NG911-specific capabilities.

- **Call Processing:** The BCF must handle all inbound calls from OSPs and should be configured between the ESInet and any interconnected ESInets to facilitate external connections.
- **Call Egress:** While optional, a BCF to manage outgoing communications between the ESInet and a PSAP may be necessary.
- **Security Features:** The BCF must incorporate the Bad Actor and Call Suspicion mechanisms as specified in NENA-STA-010.3. Calls directed to the ESInet should be accepted unless the source is blocklisted as a Bad Actor.
- **Media Handling:** The BCF must not anchor media unless it is necessary to do so. If the BCF does anchor media, it must implement ICE, STUN, and TURN mechanisms to navigate Network Address Translation (NAT) as applicable.
- **Logging and Monitoring:** The BCF must facilitate media logging per NENA-STA-010.3 specifications, with the ability to disable logging while retaining swift reactivation capabilities for diagnostic purposes.

The BCF must:

- Addresses on BCFs receiving traffic shall be globally routable IP addresses
- Process all calls from OSPs on the ingress side
- Support Bad Actor and Call Suspicion mechanisms
- Mitigate DDoS/TDoS attacks up to terabit capacity levels
- Accept calls directed to the ESInet regardless of source (unless marked as Bad Actor)
- Implement B2BUA if calls do not support REFER
- Avoid media anchoring where possible and implement ICE, STUN, and TURN when necessary
- Support ElementState and ServiceState SUBSCRIBE/NOTIFY

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 preferably from commercial SBC, Firewall, and NG911 capabilities.
- Handling inbound calls from OSPs and between ESInets; optional egress BCF for outgoing to PSAP.
- Bad Actor/Call Suspicion mechanisms; acceptance of calls unless blocklisted.
- No media anchoring unless necessary with ICE/STUN/TURN for NAT.
- Media logging per standard with disable/reactivate capabilities.
- DDoS/TDoS mitigation up to terabit levels.
- B2BUA for non-REFER calls.
- ElementState/ServiceState support.

- Descriptions of BCF locations, Bad Actor/Call Suspicion implementation, DDoS/TDoS capacity, B2BUA details, tromboning avoidance, ICE/STUN/TURN, media recording, and ElementState/ServiceState support.

2.1.2. STIR/SHAKEN Support

The State requires that incoming calls be validated, and the attestation results be supplied to PSAPs as specified in NENA-STA-010.3. Additionally, calls placed through the OCIF must be signed and receive A-level attestation when validated by the terminating service provider.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Validation of incoming calls with attestation to PSAPs per NENA-STA-010.3.
- Signing OCIF calls for A-level attestation.
- Explanation of STIR/SHAKEN implementation/conformance.

2.1.3. Security Mechanisms

Until the PCA exists, the Contractor shall provide a Certificate Authority with a certificate traceable to a Certificate Authority trusted in mainstream browsers. All NGCS components must conform to NENA-STA-010.3 and NENA-STA-040.2 security requirements:

- All transactions across the ESInet (including local area network connections at NGCS sites) shall be encrypted as required in NENA-STA-010.3.
- Every entity must have credentials traceable to the PSAP Certificate Authority (PCA) as trusted root
- All TCP transactions must use TLS with mutual authentication
- Minimum cipher suite as specified in NENA-STA-010.3, with TLS 1.3 support required
- Server Name Indication support required in all systems
- All SIP "hops" within the ESInet must use TLS with mutual authentication
- Data access must conform to owner's Data Rights Management policy
- Single Sign On (SSO) mechanism with SAML authorization required
- No sharing of credentials permitted
- Public-facing connections require additional protection against security attacks
- JWS signatures required for policies and log events
- SIP transactions from OSPs at the BCF shall have appropriately strong minimum cipher suite.
- The Contractor shall notify the State if an OSP cannot support a cipher suite minimally acceptable to the Contractor.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 security with PCA-traceable credentials as trusted root.
- Mutual TLS for TCP transactions with minimum cipher suite and TLS 1.3 support.
- Server Name Indication support; TLS with mutual authentication for SIP hops in ESInet.
- Data access per owner's DRM policy.
- SSO with SAML authorization; no credential sharing.
- Additional protection for public-facing connections.
- JWS signatures for policies/log events.
- Descriptions of PCA implementation/traceability, TLS mutual authentication, cipher suite compliance, TLS 1.3 support, Server Name Indication, and SIP hop security.

2.2. Core Routing and Location

2.2.1. Emergency Services Routing Proxy (ESRP)

The ESRP must conform to NENA-STA-010.3 standards and function as both originating and terminating ESRP. It shall be possible for a region or group of PSAPs to provide a terminating ESRP to which the State's ESRP must route calls to as appropriate.

The proposed solution must utilize the PRF functionality to support the ability to dynamically change the primary, alternate, and contingent routes available by the ESRP. The ESRP shall retrieve rule sets from a Policy Store using the NENA-STA-010.3 proscribed Policy Store web service. The ESRP must be capable of being provisioned to use any Policy Store conforming to NENA-STA-010.3. The ESRP shall implement the test call condition modifications described in NENA-STA-010.3 to enable automated testing of policy routing rules.

All calls must be location-routed with no ALI/MSAG-based routing. Requirements include:

- The ESRP shall be able to query any Location Information Servers using either HELD or SIP Presence.
- The ESRP shall support the QueueState and DequeueRegistration mechanisms for all queues it operates. It must support QueueState clients for queues for all PSAPs in the State.
- Policy Routing Rule function (PRF) supporting all NENA-STA-010.3 conditions and actions
- Policy retrieval from a Policy Store with dynamic updates (within 10 seconds)
- Handling at least 100 calls per second
- Support for admin calls
- Ability to query any compliant ECRF and Location Information Servers
- Support for call routing and EIDOs for any responder agency
- Implementation of overload and diversion mechanisms
- Additional Data mechanisms for routing based on call data
- ElementState and ServiceState support

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 as originating/terminating ESRP.
- Location-based routing only (no ALI/MSAG).
- PRF supporting all conditions/actions.
- Policy retrieval from Policy Store with <10s updates.
- Handling 100 calls/second.
- Admin call support.
- Querying compliant ECRF/LIS.
- Routing/EIDOs for responder agencies.
- Overload/diversion mechanisms.
- Additional Data routing; and ElementState/ServiceState support.

2.2.1.1. Policy Store

The State requires a Policy Store conforming to NENA-STA-010.3. The Policy Store must be capable of being the sole source of policies for the NGCS.

- The State **desires a flexible policy editor** that can create and modify policies conforming to NENA-STA-010.3 with an easy-to-use Graphical User Interface.
- The Policy Store **must have the capacity to support policies for all PSAPs and all elements in the NGCS** at the peak call rates specified in this RFS.
- Storage and retrieval of policies must be limited by the NENA-STA-010.3 Data Rights Management mechanism.
- The Policy Store must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Policy Store per NENA-STA-010.3 as sole policy source.
- Flexible GUI policy editor.
- Capacity for all PSAPs/elements at peak rates.
- DRM-limited storage/retrieval.

- ElementState/ServiceState support with State subscription.
- Detailed Policy Store description.

2.2.2. Location Information Server (LIS)

The State utilizes a Location Information Server (LIS) provided by the existing service provider. Respondents must provide a description of their LIS solution in conformance with NENA-STA-010.3.

- The LIS must supply location in the form of a PIDF-LO (location by value) or a location URI (location by reference).
- The LIS must also provide a dereference service for a location URI it supplies given the URI, the LIS provides the location value as a PIDF-LO.
- A LIS may be a database, or may be a protocol interworking function to an access network-specific protocol.
- If the LIS supply's location by reference, it must also provide dereferencing service for that location URI.
- Elements in the ESInet, including the ESRP, and the PSAP may dereference a location URI as part of processing a call.
- The LIS must support HELD, HELD Dereferencing and/or SIP Presence Event Package.
- The SIP Presence SUBSCRIBE/NOTIFY mechanism can control repeated dereferencing, especially when tracking of the caller is needed. However, HELD is acceptable on any location URI.
- The LIS must support location filters and event rate control.

The LIS may support SIP Presence to provide location-by-reference as defined by RFC 5808. Using SIP Presence, the entity desiring location subscribes to the SIP Presence Event Package at the location URI provided containing a PIDF (Presence Information Data Format) document that will include the location in the Location Object (LO) part, forming the PIDF-LO.

- The LIS may validate locations prior to entering them into the LIS using the LVF.
- The LIS may support the validation of location around planned changes as defined by draft-ecrit-lost-planned-changes[1].
- The LIS must accept credentials traceable to the PCA for authenticating queries for a location dereference. Since calls may be diverted to any available PSAP, the LIS cannot rely on any other credential source to authorize location dereferencing.
- Storage and Retrieval of location data must be controlled by the NENA-STA-010.3 Data Rights Management mechanism

When location is provided by reference there is a need for the reference to be valid, at least for the length of the call. Since the call may be transferred to a transfer-to PSAP for handling, the transfer-to PSAP must have the ability to dereference the location reference provided with the call. It is therefore critical that the location URI does not expire before the transfer-to PSAP has the opportunity to dereference it.

Any LIS that provides a dereferencing service for a location must provide an expiration time associated with that URI set at a minimum of 30 minutes, with a maximum of 24 hours.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LIS per NENA-STA-010.3 providing PIDF-LO or location URI with dereference service.
- As database or protocol interworking.
- HELD/dereferencing/SIP Presence support.
- Location filters/event rate control.
- SIP Presence for location-by-reference per RFC.
- Validation via LVF; support for planned changes draft.
- PCA-traceable credentials for dereferencing.

[1] https://datatracker.ietf.org/doc/html/draft-ecrit-lost-planned-changes-00

- DRM-controlled storage/retrieval; and minimum 30-min/max 24-hour URI expiration.

2.2.3. Location Database (LDB)

The State requires a Location Database (LDB) solution as a core component of the Emergency Services IP Network (ESInet). Respondents must provide a detailed description of their LDB solution that is conformant with NENA standards, primarily the NENA Next Generation 911 GIS Data Model (NENA-STA-005.2). The LDB serves as the authoritative geospatial database for the Location Validation Function (LVF) and the Emergency Call Routing Function (ECRF).

- The LDB must store and manage all mandatory and conditional geospatial data layers as specified in NENA-STA-005.2, including but not limited to:
    - Public Safety Answering Point (PSAP) Boundaries
    - Emergency Service Boundaries (Law, Fire, EMS)
    - Road Centerlines
    - Site / Structure Address Points
- The LDB must interface directly with the LVF to enable validation of civic location information against the authoritative GIS data contained within it.
- The LDB must interface with the ECRF to provide the necessary geospatial data for determining the appropriate PSAP and emergency service agencies for a given dispatchable location. This location-to-service mapping MUST utilize a standard protocol, such as the Location-to-Service Translation (LoST) protocol.
- The solution must provide a secure and robust mechanism for the provisioning, aggregation, and ongoing maintenance of GIS data from various authoritative local sources (e.g., county, and municipal GIS departments). This includes tools for data normalization, quality control, and discrepancy resolution.
- The LDB must be architected for high availability and geographic redundancy to ensure uninterrupted location validation and call routing services. The system must meet stringent performance requirements for real-time query processing during emergency call handling.
- The LDB must control access for data provisioning and system queries through secure authentication and authorization mechanisms, protecting data from unauthorized access, modification, or deletion.
- Storage, management, and retrieval of location data MUST be controlled by policies consistent with NENA data security and privacy standards.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LDB conformance with the NENA-STA-005.2 GIS Data Model.
- Standard-based interfaces with the LVF and ECRF (e.g., LoST).
- Support for all required NENA GIS data layers and their lifecycle management.
- A detailed process for GIS data provisioning, aggregation, updates, and quality control.
- Description of the high-availability and redundant architecture.
- Mechanisms for secure access control for both data management and system queries.
- Tools and processes for managing data quality and resolving discrepancies from multiple sources.

2.2.4. Emergency Call Routing Function / Location Validation Function (ECRF/LVF)

The implementation requires two independent, redundant ECRFs and LVFs (one inside, one outside the ESInet) with identical data. The ECRF/LVF must support the extensions to LoST defined in NENA-STA-010.3 and the similar-location and planned-changes extensions defined in draft-ietf-ecrit-similar-location[2] and draft-ietf-ecrit-lost-planned-changes[3] (or RFCs issued based on those drafts).

Query Capability:

[2] https://datatracker.ietf.org/doc/draft-ietf-ecrit-similar-location/19/
[3] https://datatracker.ietf.org/doc/draft-ietf-ecrit-lost-planned-changes/

The external ECRF/LVF must be queryable from the public internet and by any i3 OSP, supporting both iterative and recursive queries.

Responder Types:
The system must handle up to 20 responder types and various service URNs as specified.

Data Synchronization:
Both the internal ECRF and LVF must achieve 99.999% availability, while the external ECRF must meet the same 99.999% availability SLA, and the external LVF must maintain 99.9% availability.

Performance Metrics:
The internal ECRF/LVF must handle 500 queries per second effectively, ensuring that combined services meet the specified thresholds for external queries.

Key requirements:

- External ECRF/LVF accessible from the public Internet and i3 OSPs
- Support for iterative and recursive queries
- Support for up to 20 responder and all service URNs
- LoST sync interface to National Forest Guide and interconnected ESInets
- The ECRFs and LVFs must be capable of being provisioned from an SI conforming to NENA-STA 010.3.
- Routing/validation must change within eight (8) seconds of an update via the SI.
- The internal ECRF/LVF shall be capable of handling 100 queries per second for any valid Location Information shape as specified in OGC 06-142r1.
- The external ECRF/LVF shall be capable of handling an aggregate of 5000 queries per second with any mix of civic or geo points.
- The external ECRF/LVF shall be capable of handling an aggregate 500 queries per second.
- The external ECRF/LVF shall limit transactions from the same querier to, at most, 10 per second and fewer, if it is under a sustained excessive load. If the ECRF and LVFs are combined, the combination must meet the 5000/500 rate (not twice the rate of a single service).
- 99.999% availability for internal ECRF/LVF and external ECRF
- 99.9% availability for external LVF
- Support for Spatial Interface (SI) with routing/validation updates within seconds
- Capacity to handle specified query volumes
- ElementState and ServiceState support

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Two independents are redundant ECRFs/LVFs (internal/external) with identical data.
- External queryable from public Internet/i3 OSPs with iterative/recursive support.
- Handling up to 20 responder /service URNs; LoST sync to National Forest Guide/interconnected ESInets.
- 99.999% availability for internal/external ECRF and internal LVF, 99.9% for external LVF.
- SI support with seconds-level updates.
- Capacity for 500 queries/second internal; and ElementState/ServiceState support.

2.2.5. Forest Guide

The NGCS must handle calls transferred between interconnected ESInets, maintaining Forest Guide entries for the State's ECRF and LVF, and support recursive queries for locations outside the state's service area.

If a National Forest Guide is available, the contractor must ensure the State's ECRF and LVF entries are entered promptly.

Fallback Procedures:
In scenarios where queries fall outside the State’s service area, the ECRF/LVF must initiate recursive queries to the Forest Guide.

Commercial Relationships:
Frequent and excessive queries from the same entity may not be accommodated unless a reasonable commercial relationship exists.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Handling transfers between ESInets with Forest Guide entries for State's ECRF/LVF.
- Recursive queries for out-of-area locations.
- Prompt entry into National Forest Guide if available.
- Fallback recursive queries to Forest Guide for non-State areas.
- Limitations on excessive queries without commercial relationships.

2.2.6. Service/Agency Locator (SAL)

The State requires a Service/Agency Locator function as described in NENA-STA-010.3.

- The S/AL must support at least 1000 entries.
- The S/AL must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.
- The proposal must describe how agency entries are provisioned in the S/AL.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Service/Agency Locator per NENA-STA-010.3 supporting 1000+ entries.
- ElementState/ServiceState support with State subscription.
- Descriptions of agency entry provisioning and detailed S/AL.

2.3. Data and Enrichment

2.3.1. Additional Data Repository (ADR)

The State requires an Additional Data Repository (ADR) database function.

URIs pointing to the ADR may be passed in a call, in an EIDO, or by other mechanisms. The ADR shall return an XML data structure in response to an HTTPS GET of the URI.

The ADR provided by the contractor must:

- Supply Provider Info and Service Info for all calls handled by the LNG, and any OSP that does not provide its own ADR or AdditionalData by value when it sends a call to the ESInet
- Supply any of the valid AdditionalData blocks for any location, where the URI for the AdditionalData blocks would be returned from the ECRF when searched with an urn of “urn:emergency:service:AdditionalData”

The proposal must detail how ADR records are provisioned into the repository. Storage and retrieval of S/AL records must be controlled by the NENA-STA-010.3 Data Rights Management mechanism.

A call-stateful ADR may limit the length of time that it will serve data after the end of the associated emergency call. Such a time limit shall be at least five minutes. ADRs may not have the data themselves but may know where the data can be found. The response to a dereference request can be redirected to another ADR with an HTTPS 333 response (Iterative Refer).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- ADR returning XML via HTTPS GET.
- Supplying Provider/Service Info for LNG/OSPs without own ADR.
- Valid Additional Data blocks via ECRF URI.
- Provisioning details.
- DRM-controlled storage/retrieval.
- Minimum 5-minute time limit for call-stateful ADR.

- Redirect capability via HTTPS 303.

2.4. Call Flow and Media Handling

2.4.1. Call Flow and Session Handling Requirements

The Contractor shall implement call-flow behaviors consistent with the NENA i3 call model, including processing SIP INVITE requests from access networks into the ESInet, interactions with the ESRP, location queries to LIS, LVF, and ECRF, and routing to the appropriate PSAP through gateways or Call Handling Equipment (CHE). The system must support call queuing, overflow routing, and abandonment handling.

SIP signaling and location:
Headers such as P-Asserted-Identity, Diversion, History-Info, and Geolocation shall be correctly handled, and PIDF-LO location information shall be preserved during retargeting, bridging, and transfers.

Media and additional data:

The system shall handle voice, Real-Time Text (RTT), real-time video, and additional data (for example, messaging and sensor or biometric data from caller applications) per NENA definitions, with SDP negotiation, fallback to voice-only, and transcoding as needed.

Transfers:
Support is required for warm (attended) transfers, blind transfers, and inter-PSAP transfers, preserving all call metadata, location, timestamps, and media sessions without interruption.

Identity and trust:
The system shall enforce SIP identity assertions, correctly process P-Asserted-Identity and related headers, differentiate and display validated versus unvalidated identities at the PSAP, and integrate with STIR/SHAKEN for caller authenticity.

End-to-end conformance:
The ESInet and NGCS shall manage end-to-end call flows in conformance with applicable NENA and IETF standards, including origination, routing, delivery to the appropriate PSAP, transfers, and termination, while ensuring reliable session handling for all supported media.

2.4.2. Media Quality of Service (QoS)

2.4.2.1. Audio

The proposed solution shall support high-quality, reliable audio for all emergency calls. The solution must be conformant with NENA and IETF standards for audio codecs and media transport to ensure interoperability between originating networks, the ESInet, and PSAPs.

- MOS-equivalent POLQA score of 4 minimum, 4.5 average from OSP edge to PSAP edge
- Continuous sampling of >1% of calls randomly distributed
- Capability to monitor 100% of calls between any two points for up to 5 days upon request

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- High call quality with audio MOS-equivalent POLQA score of 4 minimum/4.5 average from OSP to PSAP edge.
- Continuous sampling >1% of calls; capability to monitor 100% of calls between points for up to 5 days.
- Descriptions of end-to-end media path measurement, POLQA monitoring/measurement, and logging/reporting procedures.

2.4.2.2. Video

For video services, the proposed service must utilize MOS-equivalent PEVQ score of 4 minimum, 4.5 average from OSP edge to PSAP edge, and have continuous sampling of >1% of calls randomly distributed. They should also have the capability to monitor 100% of video calls between any two points for up to 5 days upon request.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Video MOS-equivalent PEVQ score of 4 minimum/4.5 average from OSP to PSAP edge.
- Continuous sampling >1% of calls.
- Capability to monitor 100% of video calls between points for up to 5 days; and descriptions of end-to-end video path measurement, PEVQ monitoring/measurement, and logging/reporting procedures.

2.4.2.3. Text

The State requires that text to 911 and text from 911 be supported for both legacy and NG PSAPs and OSPs.

- For NG911, text to 911 shall be provided via Message Session Relay Protocol (MSRP) using standard NENA-STA-010.3 interfaces.
- For text from 911, Contractor shall maintain an interface to a commercial text gateway.
- For Legacy PSAPs, MSRP or web interfaces to the outgoing text service are required.

Text from NG PSAPs shall be able to send MSRP to an element in the NGCS which will send SMS text using the text gateway.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 100% correct text delivery 99.99% of the time.
- Foreign language translation for all texts; and descriptions of end-to-end text path measurement, translation delivery/display, monitoring for 99.99% availability, and logging/reporting procedures.

2.4.3. Interactive Multimedia Response Service (IMRS)

The Respondent must provide a description and/or documentation that supports the requirements in this section, including IMR conforming to NENA-STA-010.3.

2.4.4. Bridge

The State requires a multimedia bridge conforming to NENA-STA-010.3. The State expressly requires the bridge to handle audio, video, MSRP and RTT.

- The State has no preference on which model (ad hoc or answer all calls at a conference aware UA), but the bridge must be able to transfer calls to and from ESInets using either model as specified in NENA-STA-010.3.
- The bridge must have capacity to maintain 20 simultaneous 3-way video calls or 100 simultaneous 3-way audio calls or a mix thereof.
- The bridge must be capable of supporting up to 6 parties (caller, call taker and up to four other parties) in any conference, with any mix of media.
- The bridge must have a mechanism to support RTT mixing when the end points do not support multiple RTT streams conforming to RFC 9071, as specified in NENA-STA-010.3.
- The bridge must support logging of media using the NENA-STA-010.3 specified mechanisms.
- The bridge must support the RFC 4575 Conference Event Package.
- The bridge must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3. The State must be able to subscribe to ServiceState and receive the standard state changes. The proposal must describe the bridge in detail.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Multimedia bridge conforming to NENA-STA-010.3 handling audio/video/MSRP/RTT.
- Support for ad hoc or answer-all models with transfers using either.
- Capacity for 20 simultaneous 3-way video or 100 audio calls (mix).
- Up to 6 parties per conference with media mix.

- RTT mixing per RFC 9071.
- Media logging per standard; RFC 4575 Conference Event Package.
- ElementState/ServiceState support.
- Detailed bridge description.

2.5. Egress and External Interfaces

2.5.1. Outgoing Call Interface Function (OCIF)

The State requires an OCIF conforming to NENA-STA-010.3. The OCIF must be capable of directing a call back of an emergency call to the OSP that originated the emergency call, offering at least the same media streams negotiated in the emergency call. The contractor must obtain appropriate identities (for example, telephone numbers) for calls sent to other service providers. Use of those identities must be controlled by the Data Rights Management system specified in NENA-STA-010.3.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- OCIF per NENA-STA-010.3 for call backs to OSP with same media streams.
- Obtaining identities for other providers controlled by DRM.
- Description of OCIF utilization for call backs with implementation/integration details.

Remainder of page intentionally blank

3. GIS and Database Services Requirements

The Contractor shall implement location-based routing and ECRF/LVF functions using GIS data that conforms to the NENA GIS Data Model (NENA-STA-006.2), including civic address points, road centerlines, PSAP boundaries, emergency service polygons, and other required layers. The GIS repository must support spatial indexing for efficient queries.

Operations and Administration:
Location information is handled by the PSAPs while the State handles the PSAP boundaries and provisioning boundaries. The proposal shall include measures to maintain the PSAP interaction and where the PSAP utilizes a vendor must not interfere or materially change the contract a PSAP currently has for GIS support.

Location conveyance:
Location data shall be transported using PIDF-LO per RFC 4119 and RFC 5139 with applicable NENA extensions. The system shall deliver location information to PSAP CHE and mapping clients via standardized NG911 interfaces, supporting both push and pull mechanisms.

Validation and determination:
Integrate LVF/LIS to validate caller-provided locations, supporting geodetic coordinates (for example, WGS84) and civic addresses, including complex scenarios such as multi-line enterprises and multi-tenant buildings with address reformatting. The ECRF shall use authoritative GIS to determine the correct ESN/PSAP, with defined fallback to default routing.

Data governance and provisioning:
The GIS system shall provide change tracking, version control, time-stamped snapshots, and automated batch or incremental updates using NENA provisioning formats (for example, GML and GeoJSON). Provide a GIS data-provisioning API and a comprehensive audit log of changes, including user, timestamp, and deltas.

Rules-based routing (RBR):
Support RBR features, including time-of-day routing, temporary boundary adjustments, alternate routing logic, and attribute-driven decisions derived from GIS layers or an integrated rules engine.

3.1. Data Management and Interfaces

3.1.1. GIS and Database Management Functionality

The contractor will utilize the PSAP and State provided data for geospatial routing from the caller to the PSAP. Management of the data will be the responsibility of the State.

The contractor will have a web interface and/or automated method to provision data and retrieve post-QA data for the use of maps and/or the computer-aided dispatch (CAD) system The contractor will ensure that an update to the system will be reflected in a change in routes (where the change does affect routes) within 5 minutes of such a change, assuming no errors are detected (online, real time update capability).

All data associated with call routing and plotting will be provided in conformance with NENA Data Model standards – NENA-STA-015.10 for remaining Legacy/Enhanced 911 systems and NENA-STA-006.2 for NG911 systems.

Originating call network operators will verify civic address location information against the NG911 GIS data using the LVF provisioned as required.

The preferred data exchange will be in Environmental System Research Institute's (ESRI) Structured Query Language (SQL) Spatial Database Engine (SDE).

The managed GIS map data will replace the traditional MSAG database as the primary database for location-based call routing and location validation (ECRF/LVF) functions within the NG911 system.

The maintenance of this GIS dataset will be completed by PSAP staff or designee It is a requirement that the discrepancy reports of the data are delivered for remediation.

The contractor will be utilizing all existing and available source data and the management and coordination necessary.

- The PSAP will be responsible for providing all GIS data used in the location routing, validation, mapping services, and maintenance of such data that are part of the contractor's system.
- The data from the PSAP will include the road centerline and address range data, address structure points, PSAP boundaries, municipal boundaries, police, fire, EMS, and medical transport boundaries and many additional GIS layers useful for display in the PSAPs. GIS data used for call routing and call locations will be provided in a NENA NG911 standard format.
- The contractor will be required to establish a working relationship with the State and to work out mutually acceptable procedures for the maintenance of these databases.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Use of PSAP GIS data for geospatial routing.
- Web interface or automated method for provisioning and retrieving post-QA data for maps.
- Reflection of PSAP updates in routes within 5 mins (online real-time).
- Data structures organized in conformance to NENA Data Model Standards – NENA-STA-015.10 and NENA-STA-006.2.
- LVF for OSP civic address verification.
- Preferred ESRI SQL SDE exchange.
- Replacement of MSAG with GIS for routing/validation.
- PSAP maintenance with contractor discrepancy reports.
- Use of existing source data.
- Responsibility for all GIS data maintenance.
- Inclusion of road centerline, address points, PSAP emergency boundaries, and additional layers.
- Mutually acceptable maintenance procedures with State.

3.1.2. Spatial Interface (SI) Functionality

The contractor will implement a Spatial Interface and ensure following capabilities are implemented:

- GIS data provisioned by the spatial interface (SI) will undergo data-quality and data-integrity checks to ensure that the data complies with all applicable requirements of NENA-STA-015.10-2018, NENA-STA-006.2-2022, NENA-02-014 and NENA-STA-010.3-2021 while maintaining the online, real time update capability.
- The SI will convert the GIS data meeting these requirements into the format (data structure and projection) used by the ECRF and LVF, in real-time or near-real-time, using a Web feature service.
- The SI will be able to provision and perform incremental updates, in near-real-time, to the ECRF, LVF, the map viewer service, the PSAP map display and similar applications that consume GIS data.
- Validation of GIS data and data updates prior to their provisioning into the ECRF and LVF, along with the means of online real-time provisioning of updates to the GIS data provisioned to the ECRF and LVF.
- The SI operation will align with the data maintenance processes with minimal impact to existing operations.
- The SI will receive and incorporate the SI datasets that have been prepared by the PSAP as previously described.
- Web interface tool for viewing and submitting incidents and change tickets.
- Web interface tool for viewing policy-routing plans.

The contractor will be able to test and then apply updates to the operating ECRF by a secure and reliable method that does not create operational problems.

The contractor's GIS functions will be able to perform database audits for common problems and errors, such as gaps, overlaps or number range conflicts, which if encountered, will be referred back to the PSAP for resolution.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SI implementation with data-quality and integrity checks per NENA standards while maintaining real-time updates.

- Conversion to ECRF/LVF format via Web feature service.
- Incremental near real-time updates to ECRF/LVF, map viewer, and PSAP displays.
- Validation prior to provisioning with online real-time updates.
- Alignment with PSAP processes.
- Incorporation of PSAP prepared datasets.
- Web tools for incidents, change tickets and policy-routing views.
- Secure reliable update and testing application without problems.
- Database audits for gaps/overlaps/conflicts referred to PSAP.

3.2. Core Data Services

3.2.1. Mapping Data Service

A Mapping Data Service conforming to NENA-STA-010.3 will be provided. This must be available within 18 months. The MDS will be capable of providing maps for all calls for all entities inside the ESInet and for calls handled out of area in other ESInets.

- The MDS must support both images and features as described in NENA-STA-010.3
- The MDS must support all layers defined in NENA-STA-006.2. Additional layers may be supported, and the proposal will describe what additional layers the MDS will support.
- Retrieval of map data must be controlled by the NENA-STA-010.3 Data Rights Management mechanism.
- The MDS must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- MDS per NENA-STA-010.3 available within 18 months for all calls/entities.
- Support for images/features.
- All layers per NENA-STA-006.2.
- Additional layers described; DRM-controlled retrieval; ElementState/ServiceState support with State subscription.

3.2.2. MSAG Conversion Service (MCS)

The MSAG Conversion Service (MCS) shall support the standard SI interface for provisioning. The proposal may include additional options that would lessen the burden on PSAPs upgrading their GIS systems to NG standards.

The State expects the LNG to support the SOA interface towards the legacy OSP, store the data in the Location Database in LVF-valid form and convert it to and from the legacy data formats using the MCS.

The State expects the LPG to support the MF/ALI interface towards the legacy PSAP, retrieve the location from a Location Information Server in LVF-valid form and convert it to and from the legacy data formats using the MCS.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An MSAG Conversion Service (MCS) conforming to NENA-STA-010.3 will be implemented.
- The MCS must support Element State and Service State SUBSCRIBE/NOTIFY per NENA-STA 010.3.
- The State must be able to subscribe to Service State and receive the standard state changes.

3.2.3. Geocode Conversion Service (GCS)

The Geocode Conversion Service (GCS) shall support the standard SI interface for provisioning. The proposal may include additional options that would lessen the burden on PSAPs upgrading their GIS systems to NG standards.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- GCS per NENA-STA-010.3 with SI provisioning (additional options for PSAP GIS upgrades).
- Return of ECRF routing location for civic addresses.
- ElementState/ServiceState support.
- ServiceState and receive the standard state changes.
- The GCS must return the same location that the ECRF uses for routing when given a civic address.

3.3. PSAP-Facing Services

3.3.1. PSAP Mapping Service

The State requires a Mapping Data Service (MDS) conforming to NENA-STA-010.3.

The services required must enable the PSAP mapping system and ECRF/LVF system to support multiple methods for reporting location errors. They include:

- ECRF civic location geocoding errors are automatically captured by the data management application utilized by the PSAP.
- LVF failures are automatically captured by the LVF and forwarded to the data management application utilized by the PSAP.
- 911 call mapping failures (calls that could not be mapped automatically) are captured by the system and forwarded to the data management application utilized by the PSAP.
- 911 telecommunicators and dispatchers may manually generate a discrepancy report, and the system can automatically forward the reports to the data management application utilized by the PSAP.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- PSAP mapping using PSAP geospatial info.
- Support for error reporting methods (ECRF geocoding errors captured.
- LVF failures forwarded; unmapped calls captured; manual discrepancy reports forwarded.

3.3.2. Map Discrepancy Reporting

The Respondent must provide a description and/or documentation that supports the requirements in this section for referral of all geospatial discrepancies to the State for remediation.

Note:
GIS-related discrepancy reporting technical requirements are detailed in §E-6.7.2, et seq. of this document.

3.4. External Integrations

The Respondent must provide a description and/or documentation that supports the integration with additional vendors as required to provide functionality to all PSAPs as currently utilized.

Remainder of page intentionally blank

4. Security Requirements

The contractor shall implement the NENA NG-SEC security and trust model, featuring strong authentication and authorization for all interfaces, mutual TLS for inter-service communications, edge security via SBCs and Back-to-Back User Agents (B2BUAs), network segmentation, and secure management planes. Threat mitigations must address Denial of Service (DoS), Distributed DoS (DDoS), Telephony Denial of Service (TDoS), SIP flooding, spoofing, and injection attacks through rate limiting, anomaly detection, and firewalls.

Implement Role-Based Access Control (RBAC) with granular permissions, multifactor authentication (MFA) for all administrative access, least privilege enforcement, and auditing of service accounts. Integration with external identity providers (e.g., SAML/OAuth) must be supported.

All location data, call content, and PII must be encrypted in transit (TLS 1.3) and at rest (AES-256 or stronger), with data minimization, pseudonymization, and compliance with laws like HIPAA and CJIS where applicable. Access to sensitive data shall require explicit consent logging.

Provide Public Key Infrastructure (PKI) processes for certificate issuance/rotation, Certificate Revocation List (CRL)/Online Certificate Status Protocol (OCSP) validation, and secure key storage using Hardware Security Modules (HSMs) or compliant vaults. Automated alerts for expiring certificates must be included.

The contractor shall supply an incident response plan aligned with NENA, including vulnerability disclosure protocols, regular patch schedules (e.g., critical patches within 30 days), and forwarding of security event logs to the jurisdiction's Security Information and Event Management (SIEM) system via secure channels (e.g., Syslog over TLS).

Provide results from independent penetration testing (conducted within the last 12 months), SSAE 18/SOC 2 audit reports, and support for jurisdiction-led security acceptance testing, including network scans, application fuzzing, and red-team exercises.

4.1. Management and Process Control

4.1.1. Personnel Roles and Responsibilities

Safeguarding NG911 assets – across **NGCS platforms** and the **ESInet** – is a shared duty. The contractor must **define, assign, and document** minimum security roles and responsibilities, whether performed internally or by external providers. At a minimum, the following roles must be covered by **named, accountable** individuals. Where third parties perform duties (carriers, cloud, managed services, subcontractors), the contractor remains responsible for assignment and verification.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An organizational roles matrix (e.g., org chart and/or RACI) identifying named individuals (or positions) for: Security Manager, Security Administrator, Data Owner(s), Data Custodian(s), Data User populations, and Security Audit Manager. Note any shared/combined roles and the accountable individual for each responsibility. Map these to NGCS components and ESInet segments.
- Documented role definitions aligned to the duties above, including authorities (e.g., the Security Manager's authority to set security policy for all NGCS/ESInet components; Security Administrator authority to implement and enforce controls across applications, network, cloud).
- Evidence that personnel are informed of their roles and responsibilities (e.g., acknowledgement forms, training records, onboarding materials, policy attestations).
- A data ownership register mapping every NG911 data set (local and remote) to a Data Owner; include classification and handling responsibilities.
- A data custodianship register mapping every NG911 data set (at rest and in transit, local and remote) to a Data Custodian; include the operational security measures they manage (encryption, key management touchpoints, access administration, backup/restore).
- Security administration procedures showing how the Security Administrator implements and maintains security controls in accordance with NG911 policies – for NGCS applications, the ESInet, edge devices, and management portals).

- An audit governance plan for the Security Audit Manager covering periodic audit cadence (internal/external), scope, reporting, and risk rating of findings, and tracking to closure.
- Role coverage procedures (e.g., delegation during absence) ensuring continuity while preserving single-point accountability for each required responsibility.
- If external parties are involved, contractual or policy evidence assigning role responsibilities to vendors/contractors/subcontractors and showing how the prime provider verifies fulfillment (e.g., attestations, SLAs, right-to-audit).

4.1.2. Identity Management

The contractor must operate a standards-based **Public Key Infrastructure (PKI)** to uniquely identify and authenticate every participating **agency** and **agent** across all NGCS and ESInet interfaces. An agency's identity must be a globally unique **FQDN** (e.g., `erie.psap.ny.us`) encoded in the X.509 `SubjectAltName` **(SAN)**. An agent's identity must use the `user@agencyfqdn` format (e.g., `nancy@erie.psap.ny.us`) and be encoded in the SAN of the agent certificate.

For PSAPs and 911 Authorities, the **PSAP Credentialing Agency (PCA)** is the **root of trust** for agency and agent certificates. The trust chain may include **national → state → agency/PSAP CAs**. Issuance may be performed directly by the PCA or by approved subordinate CAs under that chain. Any issuing authority must operate under a formal **Certificate Policy/Certification Practice Statement (CP/CPS)** with documented identity proofing and issuance controls. If an agency cannot meet those controls, it must use a **managed CA** that enforces the CP/CPS.

Private keys must be safeguarded in **FIPS 140-2** validated cryptographic modules at these minimum levels: **Level 2** for agency private keys (**Level 3 preferred**), **Level 3** for agency CA keys, and **Level 4** for state/national CA keys. **Certificate-based authentication (e.g., mTLS)** must be enforced so that valid identities and credentials are required for access to **all** NGCS/ESInet services and data (e.g., SIP signaling, APIs, management portals, interconnects).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An identity and certificate schema showing agency FQDN conventions and agent identifier format (`user@agencyfqdn`), with confirmation these identifiers appear in X.509 SAN fields for agency and agent certificates.
- A PCA/PKI trust architecture (diagram & narrative) showing the PCA root, any national → state → agency CA tiers, and permitted subordinate issuing models (e.g., PSAP/Authority issuing agent certs).
- A current CP/CPS (or binding reference) for each issuing authority, defining identity proofing, issuance, renewal, revocation, auditing, and key management; state who operates each CA (Respondent, State, third party) and how compliance is enforced.
- Key protection evidence demonstrating FIPS 140-2 validation and deployment at required levels:
    - Agency private keys: Level 2 minimum (note if Level 3 is implemented).
    - Agency CA keys: Level 3
    - State/National CA keys: Level 4
- Key protection evidence should include device inventories, validation certificates, hosting locations, and any escrow arrangements.
- Access control enforcement description confirming certificate-based authentication (e.g., mTLS) is required for all NGCS/ESInet services and data, where enforcement occurs (interfaces, APIs, signaling paths), and how failed, expired, or revoked certificates are detected and blocked.
- Certificate profiles and samples (agency and agent): SAN contents, Key Usage/EKU, validity periods, revocation mechanisms (CRL/OCSP), and sample chains validating to the PCA.
- Operational lifecycle procedures for issuance, renewal, suspension/revocation, replacement, and compromise response; include joiner/mover/leaver workflows for agents and rollover plans for CA keys.
- Contingency approach if an entity cannot securely operate a CA (e.g., use of a managed CA aligned to the CP/CPS), including contractual controls, SLAs/SLOs, and audit rights.

4.1.2.1. Roles

Every **agency** and **agent** must authenticate with an X.509 certificate that asserts one or more roles used for authorization.

- **Agency roles** define organizational authority, optionally constrained by **scope**.
- **Agent roles** define individual privileges and may include **modifiers** as identified in NENA-STA-010.3 §5.3.

Role assignment for any agency or agent must be **approved and limited by the immediately superior agency's policy**. Solutions may support local roles, but **full functionality must work with baseline roles and scopes** for mutual aid and roaming. Roles must be **encoded in certificates** (role OIDs/attributes per profile) and **enforced at NGCS/ESInet interfaces**.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A role model and governance describing agency role, agent roles, and allowed scopes, including how the immediately superior agency approves/limits assignments and how those policies are enforced.
- Role encoding specification for X.509 showing exactly how roles/modifiers/scopes are carried (e.g., OIDs or SAN/subject attributes) with minimal sample certs limited to the role fields and a description of validation during authentication.
- An authorization design that consumes certificate-asserted roles to make access decisions across NGCS/ESInet services, with least-privilege mappings from each role (and modifier) to permissions.
- Evidence of baseline role coverage showing agencies exist that assume all baseline agency roles and that no custom roles are required for full system functionality.
- A role registry integration plan (reference NENA-STA-010.3 §10.27 & §10.28) describing how the solution references the Agency and Agent Role registries, maps them to authorization objects, and process registry updates.
- Role lifecycle controls: request to and approval by the superior agency, assignment changes, revocation, and timely de-provisioning; include joiner/mover/leaver workflows for agents' roles.
- Operational procedures for modifiers showing how modifiers adjust privileges without creating new base roles.
- Monitoring and audit showing how role use is logged, reviewed, and tied back to the approving superior agency; include alerts for unauthorized role elevation.
- Exception handling for temporary/emergency role increases: approval, time bounds, logging, and revocation; include how conflicts between local custom roles and baseline roles are resolved while keeping services available.

4.1.3. Policies and Procedures

The contractor must maintain a comprehensive cybersecurity policy framework for **NGCS platforms** and the **ESInet**. Policies may be separate or consolidated, but each required area must have clear **purpose, scope, roles, approval, version control, distribution, and compliance expectations**. Policies must be **approved**, **communicated to personnel**, and **reviewed and/or updated on a defined cadence** (at least annually or upon material change) to reflect new and emerging technologies, threats, and processes.

Policies must **flow down** to vendors/contractors/subcontractors and be backed by **Standard Operating Procedures (SOPs)** that turn policy into repeatable tasks. (e.g., user onboarding, vendor remote access, incident handling, recovery). SOPs must be created, kept current, and used in daily operations.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Policy governance covering ownership, approval authority, versioning, distribution/acknowledgement, training, and review/update cadence.
- A policy inventory (or consolidated policy) including, at minimum, the policies identified in NENA-STA-040.2 §4.1.2.

- Contractual flow-down language proving applicable policies bind all vendors, contractors, and subcontractors supporting NGCS/ESInet.
- A complete SOP catalog mapped to the above policies.
- SOP governance describing authorship, approval, version control, authoritative storage, and periodic update cycle; include triggers for out-of-band updates (e.g., new technology implementation or threat vectors)
- Training and attestation evidence showing personnel have been informed of relevant policies and procedures.
- Compliance and exception processes describing how adherence is monitored; how exceptions/waivers are requested, risk-assessed, time-bounded, approved; and how they are revisited/closed.
- Cross-references showing how policies and SOPs align with the Risk Management program and Incident Response, ensuring non-compliance items route to corrective action and/or formal risk acceptance.

4.1.3.1. Incident Response Plans

Early detection and disciplined response are essential to protect NG911 operations. Detection should use tooling (e.g., SIEM, IDS/IPS) and informed personnel, with trained staff triaging scope and impact. The contractor must maintain a formal, written **Cybersecurity Incident Response Plan (CIRP)** that is adaptable, periodically evaluated and tested, and staffed by trained responders. The CIRP should follow **Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity** and define when and how to engage external resources.

Because NG911 must continue answering calls and dispatching responders even under attack, recovery planning must be rigorous. The contractor must maintain **Business Continuity (BC)** and **Disaster Recovery (DR)** plans (separate or combined; separate recommended), store all plans offline yet accessible to recovery teams, and review/test at least annually, updating plans as needed.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A CIRP aligned to Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity, with incident declaration/classification criteria and communications/notification procedures.
- Detection capabilities and processes showing how SIEM, IDS/IPS, and staff reports enable early detection; include triage workflows, severity classification, and criteria to escalate to incident status.
- Training and exercise evidence for personnel with plan duties and proof the CIRP is tested (tabletop/live); include after-action reviews and documented improvements.
- A Business Continuity (BC) Plan for maintaining critical services during and after disruption.
- A Disaster Recovery (DR) Plan detailing IT restoration and coordination with ongoing mission-critical operations.
- Plan maintenance & accessibility controls proving CIRP/BC/DR are maintained offline yet readily accessible to recovery teams, with clear ownership, version control, and distribution.
- Review and test cadence showing at least annual reviews/tests of CIRP/BC/DR, with triggers for interim updates and documented results.
- Containment and recovery playbooks/SOPs translating plans into actionable steps for common scenarios (malware/ransomware, denial of service, critical service outage), including initial containment, eradication, service restoration, and lessons learned.
- External assistance procedures specifying when/how outside help is engaged, required approvals, and current contact lists/resources.

4.1.4. Authorization and Data Rights Management

The contractor must enforce **XACML 2.0-based authorization** for all NG911 interfaces and protected data. Policies must evaluate **subject, resource, action, and context attributes**; be stored in a **Policy Store** (§E-2.2.1.1); decided by a **Policy Decision Point (PDP)**; and enforced at a **Policy Enforcement Point (PEP)**. Interfaces and data must use

consistent names (NENA-STA-010.3 §10, et seq.). Actions must be explicit – **Read, Create, Update, Delete, Execute** – with **permit/deny rules** and an **explicit default rule** for every policy set.

Provisioning data is owned by the agency that operates the element and must be governed by **data rights management**. Each XACML policy must be **packaged as a JWS** and **signed by the policy owner**, including the **signing certificate and full chain** for validation.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Authorization architecture showing XACML 2.0 components, PDP placement, and how authorization is invoked on all NGCS/ESInet interfaces and protected data paths.
- Policy naming conventions & registries usage, including:
  - Interface policy names derived from `ServiceID`, and an interface keyword (NENA-STA-010.3 §10.30) formatted `ServiceID~keyword` (e.g., `LoST~ecrf.state.pa.us`)
  - Data item names derived from OpenAPI JSON object names and optional element tags, using dot notation (e.g., `civicAddr.A3`, or `<eido.AgencyDataComponent.AgencyName>`)
  - Mapping to the Policy Type Registry (NENA-STA-010.3 §10.33)
- Action model defining Read, Create, Update, Delete, Execute, with examples showing how each applies to representative Interfaces and data structures.
- Example XACML policy sets for:
  - One or more interfaces
  - One or more data structures
  - Each example policy set provided must include permit/deny rules, an explicit default rule, and attribute conditions (subject/resource/action/date/time as applicable).
- JWS packaging & validation: how the policy owner signs policies; how the certificate and chain are included (by value or reference); how PEP/PDP validate signatures (CRL/OCSP) and how key rotation and revocation are handled.
- Data rights management procedures establishing ownership of provisioning data and how ownership is enforced in policy.
- Policy lifecycle controls: authoring, peer review, change management, pre-production testing/evaluation, promotion, versioning, rollback, archival; include who is authorized to sign and publish policies.
- Logging & auditability: decision logs at PEP/PDP, retention, and procedures for reviewing denied/exception events.
- Performance & availability targets: PDP availability/latency, decision/policy caching (TTL/invalidations), and fail-secure behavior if policies or validators are unavailable.

4.2. Information System Infrastructure and Management

4.2.1. Device Inventory

The contractor must maintain a **continuously updated inventory** of all **devices, software/applications, software libraries, data sets, and cloud/third-party services** that support the NGCS platform and the ESInet. Use automated discovery and reconciliation where possible to keep records accurate, quickly identify unauthorized items, verify patch/firmware levels, and support zoning/segmentation. If full visibility is limited by span of control or contracts, clearly define what is in scope, assumptions, and responsibilities. Inventory outputs must inform critical impact analysis (BC/DR inputs) and drive trusted vs. untrusted zone design and controls at all ingress/egress points.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Inventory management approach describing data sources, automated discovery tools/processes (where used), manual reconciliation, update frequency, and how unauthorized/unknown items are identified and removed or quarantined.
- Scope and span-of-control statement clarifying which assets/services fall under the Provider vs. the Customer or other vendors; include contractual boundaries, dependencies, and any blind spots.
- Comprehensive inventory documentation should identify sufficient detail – at minimum, documenting inventory elements identified in NENA-STA-040.2 §5.4 – for all aspects of NGCS and ESInet infrastructure.

- Classification linkage showing how inventories map to the provider's data classification policy and define required protections.
- Impact analysis methodology showing how the inventory feeds critical impact analysis and integrates with Business Continuity and Disaster Recovery planning
- Zoning/segmentation mapping that uses the inventory to define trusted vs. untrusted zones and sets control placement and rule scope at all ingress/egress points.
- Governance & lifecycle controls for the inventory: ownership, update cadence, audit/attestation of accuracy, change triggers, reconciliation with change management processes, and evidence of periodic cleanup of stale records.

4.2.2. Patching and Update Management

The contractor must implement a disciplined, **change-managed patching program** covering **firmware, hardware drivers, operating systems, applications, and middleware**. The program must take in vendor, CERT, or other security advisories, use a common severity scale (e.g., Common Vulnerability Scoring System [CVSS]) to set priority, and check the environment for indicators of compromise (IoC) when a vulnerability is disclosed. Patching must be timely and paired with post-patch verification. The program should align with timelines and processes defined in NENA-STA-040.2 §5.5.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A process to validate – at least monthly – that all required patches are installed across in-scope hardware and software (plus event-driven checks upon major vulnerability disclosures).
- A change-managed deployment workflow ensuring approved and appropriately tested mitigations/patches are applied as soon as possible, with defined rollback steps.
- Post-patch verification to confirm remediation and to check for exploitation and/or other IoCs across the ESInet and NGCS.
- A CVSS-based timeline policy that sets SLAs by severity/criticality (e.g., critical expedited; target $\leq$ 48 hours from disclosure or patch availability), and an emergency change path.
- Evidence of advisory intake and triage, including how severity, affected scope, available mitigations, and permanent vs. temporary fixes are evaluated and tracked.
- Exception handling with compensating controls when patches cannot be applied immediately, with documented risk acceptance under the Entity's risk management process.
- Reporting and metrics showing patch compliance, age of open findings by CVSS band, time-to-patch, and reconciliation with the inventory/CMDB to ensure complete coverage.

4.2.3. Segmentation and Traffic Separation

The contractor must implement **domain-level network segmentation** to contain incidents, reduce lateral movement, and improve resiliency. Segmentation may be physical or logical (e.g., firewall-enforced choke points) and should extend to **zero-trust/micro-segmentation** at the endpoint or workload wherever feasible. Production and non-production (test/training) must be strictly separated so non-production activity cannot affect production services. **Development tools are prohibited in the production environment.** Within each environment, distinct traffic classes (e.g., call/signaling, management/monitoring, administrative) must be segregated and filtered (VLANs and/or dedicated equipment) with explicit allow-lists and firewall policy. Management/monitoring traffic must be out-of-band, normal traffic must not use the default VLAN, and configuration access to traffic-handling devices must use administrator-level accounts under appropriate controls.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A segmentation architecture showing production vs. non-production separation, inter-segment demarcation points, and isolation/containment controls.
- A traffic separation design identifying major traffic classes and how they are segregated and filtered.

- Evidence that production is protected from non-production, including controls preventing any non-production impact on production systems, and an explicit statement that no development tools exist in the production environment.
- Out-of-band management/monitoring implementation details and confirmation that normal traffic is not on the default VLAN.
- Administrative access controls for traffic-handling devices: administrator-level account use, authorization model, MFA, logging, and audit.
- Operational procedures/SOPs for change, testing, and validation of segmentation and filtering rules, including onboarding of new services without weakening isolation.
- Monitoring & alerting for policy violation and lateral movement detection within/across segments, with procedures for rapid containment.

4.2.4. Network Boundary Protection

Firewalls and Next Generation Firewalls (NGFWs) are key perimeter and inter-segment controls, but they are not the only defense. Internal systems must also be secure. The contractor must deploy a NENA-standard Border Control Function (BCF) or other boundary protections at all ESInet ingress/egress points and each segment entry/exit using explicit allow-lists that document required traffic and block all else. Specific BCF behaviors and requirements are identified in §E-2.1.1 of this document.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A boundary architecture showing boundary controls (BCF or NGFW) at all ESInet ingress and segment entry/exit. The BCF must conform to requirements in §E-2.1.1 of this document.
- A traffic matrix for each firewall listing required services, ports, and protocols, with explicit allow rules; unnecessary traffic must be blocked by default.
- Performance & availability: high availability (HA) and/or failover capability, and traffic inspection features must be configured so boundary protections do not degrade service delivery capabilities.

4.2.4.1. External Connections

NG911 relies on external connections; with these links often traversing the public internet, they must follow a zero-trust approach (NENA-STA-040.2 Appendix A & NIST Special Publication 800-207) and use layered protections. At minimum, each external connection must be protected by a boundary protection device conforming to requirements identified in §E-5.2.4 above, and any connection transporting sensitive information must use an encryption that conforms with the requirements identified in NENA-STA-040.2 §4.2.2.6 (Safeguarding Sensitive Electronic Information).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An external connectivity architecture listing counterparties, paths, and media, and how zero-trust principles are applied.
- Evidence that all external links are protected by a firewall with placement, explicit allow-lists, and default-deny posture per §E-5.2.4.
- An encryption approach for links carrying sensitive information, conforming to requirements of NENA-STA-040.2 §4.2.2.6, indicating where encryption is enforced.
- Operational controls for onboarding/approval, continuous monitoring, periodic review, and change/termination of external connections – consistent with zero-trust and boundary protection requirements.

4.2.4.2. Demilitarized Zones (DMZ)

Some NG911 services must be reachable from untrusted networks. Any externally accessible resource not otherwise protected by equivalent controls must reside in a Demilitarized Zone (DMZ) that is segments from internal NGCS/ESInet segments and mediated by a boundary protection device per §E-5.2.4 of this document.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DMZ architecture showing externally accessible resources, segmentation from internal networks, and firewall/SBC/BCF demarcation points.
- A traffic controls strategy for the DMZ: default-deny posture, explicit allow lists, tightly limited ingress/egress, and no lateral access to internal segments.
- Hardening & monitoring for DMZ assets: patch cadence, configuration baselines, centralized logging, telemetry, and alerting.
- Operational procedures for onboarding and retiring DMZ-hosted services, plus periodic reviews to confirm resources that require external access remain correctly isolated in the DMZ.

4.2.4.3. Defense in Depth

The contractor must apply Defense in Depth (DiD) – layered, overlapping controls that protect confidentiality, integrity, and availability across physical access, endpoints, data protection, boundary defenses, network and traffic separation, system monitoring, and (where applicable) vendor diversity. DiD ensures that if one control fails, others maintain security. Critical systems and sensitive information shall utilize Defense in Depth with deliberate redundancy and no single points of failure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DiD architecture showing layered controls across the stack: physical access, endpoints, identity/authorization/authentication, boundary protections, and segmentation/traffic separation.
- A control-to-risk mapping for critical systems and sensitive data identifying how multiple independent controls address key threats, with no single-control dependencies.
- Failure mode and fallback analysis demonstrating how security is maintained if a layer is bypassed or fails.
- Operational integration with related sections (e.g., IAM/roles, segmentation, boundary protections, incident response, logging/monitoring), including runbooks for escalation between layers.
- Validation and review evidence and metrics showing layered control effectiveness over time.

4.2.4.4. Remote Access

Remote access connects users to systems outside a physical location. External remote access carries the highest risk and must be allowed only for documented business need, routed through authorized, secured, encrypted connections (e.g., VPN aligned to NIST SP 800-77), and enforced with strong authentication and centralized logging.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Access control & eligibility: Processes ensuring external remote access is granted only for valid business need, with at least annual account reviews and timely removal when no longer required.
- Secure connectivity: Use of an authorized, encrypted connection for all external remote access. MFA must be implemented for all remote connectivity.
- Operational governance: SOPs for requesting, approving, establishing, and terminating remote access, plus periodic tests/reviews to confirm controls remain effective.
- Logging & monitoring: centralized logging for remote connectivity in conformance with minimum requirements identified in NENA-STA-040.2 §6.17.

4.2.5. Infrastructure Resilience

Mission-critical NG911 functions must remain available despite single-component failures and localized outages. The contractor must employ redundancy and diversity across the ESInet and NGCS, through the deployment of high-availability mechanisms with supported infrastructure where appropriate. Because infrastructure failures can drop in-progress sessions, applications and signaling must gracefully recover during a path or site failure. NGCS/ESInet

components must be both redundant and diverse, and ingress traffic must enter the NG911 system through diverse paths. (Additional redundancy guidance in NENA-STA-010.3 §2.9)

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An end-to-end High Availability (HA) architecture showing redundant components and physically diverse ingress/egress, transport, facilities, and power; include call/signaling paths proving diverse 911 call entry.
- Component-level HA designs with health checks, failover criteria, and state synchronization.
- A diversity plan detailing route/provider diversity, facility/region separation, and power diversity.
- Application/session continuity methods that demonstrate graceful recovery during device/site failover.
- Testing & exercise evidence for failover/fallback, with measured recovery objectives and tracked corrective actions.
- Operations & monitoring for infrastructure health; maintenance procedures that avoid creating single points of failure during changes, and SOPs for failure scenarios.

4.3. Authentication and Federated SSO

Agent authentication across NG911 must use federated Single Sign-On (SSO) based on OASIS SAML v2.0. Identity Providers (IdPs) authenticate agents and issues assertions to Relying Parties (RPs) for authorization. For HTTP-bound apps, IdPs and RPs must support Web Browser SSO, Identity Provider Discovery, and Single Logout; ECP and Artifact Resolution may be supported. SAML metadata should be aggregated under one `<EntitiesDescriptor>` and digitally signed by an identified administrative body using a well-known certificate to bootstrap trust.

For session establishment between agents and elements, SSO authenticates the agent and unlocks the agent's private key; the agent's X.509 certificate is then used to form the TLS session. For SIP and HTTPS, mutual TLS (mTLS) must be used with certificates traceable to the PCA for agents, agencies, and elements. RSA-2048 must be supported and accepted and accepted ESInet-wide (alternatives may be accepted only if cryptographically equivalent to, or stronger than RSA-2048). Each IdP must enforce multifactor authentication (MFA) for agents using a combination of at least two (additional factors preferred) of the following: password, token, smart card, or biometrics. Offline or other locally available backup authentication methods should be implemented for use if network access to primary authentication methods is unavailable.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An SSO architecture showing IdP(s), RPs, and assertion flows; conform all agent operations requiring authorization rely on SAML v2.0
- mTLS designs for SIP and HTTPS using PCA-traceable certificates for agents, agencies, and elements; include trust anchors, path validation, and revocation checks.
- A cryptographic baseline confirming RSA-2048 support and acceptance ESInet-wide and policy for accepting alternatives only if equivalent to, or stronger than RSA-2048.
- IdP MFA enforcement: supported factors, enrollment of multiple factors, and backup local authentication.
- The TLS establishment flow where SSO authentication unlocks the agent's private key used with the agent's certificate to negotiate the TLS session.
- Operational controls: onboarding/offboarding, key & certificate lifecycle, assertion & metadata signing key rotation, and monitoring/logging of authentication events.

4.4. Cryptography and Public Key Infrastructure

Cryptography in NG911 primarily secures connections and proves identity: asymmetric keys/X.509 certificates authenticate endpoints and establish sessions; symmetric ciphers then protect data in transit. The NG911 PKI is PCA-rooted: the PSAP Credentialing Agency (PCA) issues subordinate CA certificates to ESInet-operated Intermediate CAs (ICAs). Approved ICAs may, in turn, issue end-entity certificates to NGCS/ESInet service elements, and personnel. Full controlling specifications for the NG911 PKI are: NG911 Interoperability Oversight Commission (NIOC) PSAP Credentialing Agency Certificate Policy, and NIOC PSAP Credentialing Agency Certificate Validation Policy.

(section continues next page)

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- PKI trust architecture showing the PCA root, Contractor-operated ICA(s), end-entity certificate issuance, and provision for subordinate ICA implementation and certificate issuance.
- Operational practices for certificate lifecycle and key management, including how asymmetric authentication bootstraps TLS/mTLS and how symmetric session keys are negotiated.
- Certificate profiles & example chains demonstrating path validation to the PCA, with revocation checking and trust-anchor management
- Conformance statements confirming acceptance of PCA-rooted RSA-compatible credentials, consistent with the controlling specifications from the NIOC PCA Certificate Policy and NIOC PCA Certificate Validation Policy.
- TLS alignment: where and how TLS/mTLS is enforced across NGCS/ESInet interfaces showing asymmetric establishment and symmetric protection in session.

4.4.1. Cryptographic Keys

Cryptographic keys underpin identity and data protection in NG911. Keys are algorithm-specific and generated by approved processes. For asymmetric key pairs, the public key is submitted to a CA for inclusion in an X.509 certificate and the private key is securely stored. Private and symmetric keys must be protected against loss, corruption, and unauthorized access, with periodic access reviews. Private keys should be classified as 'Sensitive (Most Sensitive Information)' in alignment with NENA-STA-040.2 §4.2.2.1.4, or at a comparable level that aligns with the contractor's existing data classification schema. Private keys must be revoked and reissued if compromised, or if compromised is suspected. Cryptographic key implementations must adhere to the NIOC PCA Certificate Policy and NIOC PCA Validation Policy and align with the NENA i3 Standard (NENA-STA-010.3) and NIST SP 800-57 Part 2 Rev. 1 (Recommendation for Key Management: Part 2: Best Practices for Key Management Organizations).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Key generation & issuance procedures: how keys are generated, how public keys are submitted to the CA, and where/how private keys are stored.
- A classification statement designating private keys as 'Sensitive (Most Sensitive Information),' or similar, and the technical/administrative controls that enforce this classification.
- Access control & periodic review: who/what can access keys, authentication required, separation of duties, and the cadence/mechanics of access recertification.
- Key protection measures for storage/backup/restore, including protections at rest and in use, and configuration practices consistent with current TLS guidance.
- A compromise response plan detailing detection, revocation, re-issuance, distribution, and restoration steps when keys are, or suspected to be, compromised.
- Lifecycle management covering creation, distribution, rotation, archival and destruction, with logging/audit trails sufficient for compliance and forensics.
- Conformance attestations to the NIOC PCA Certificate Policy and NIOC PCA Validation Policy.

4.4.2. Use of Self-Signed Certificates

Self-signed certificates MUST NOT be used for any NG911 communications that traverse an ESInet. All communications must use certificates traceable to the PCA root. External entities that are not in the PCA-traceable PKI must present certificated issued by a reputable public Certificate Authority. This ensures peer identity is validated through a recognized trust chain and prevents unauthenticated endpoints from participating in NG911 exchanges.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A certificate policy and enforcement plan affirming no self-signed certificates within or between ESInets and that NGCS/PSAP elements use PCA-anchored certificates.
- External entity onboarding requirements stating non-PCA participants must use Public CA certificates, and how this is verified during trust establishment.

- Trust store and path-validation configuration for SIP, HTTPS, APIs, and management interfaces, accepting only PCA-anchored chains (or approved public CA chains) with CRL/OSCP checks.
- An asset/certificate inventory and automated detection controls to identify and block self-signed or untrusted certs.
- An exception policy confirming there are no exceptions for self-signed certificates on ESInet-traversing communication, including test and non-production environments.

4.5. Integrity Protection

All NG 911 protocol operations must be integrity-protected with TLS, using SHA-256 or stronger (FIPS PUB 180-4); SHA-256 must be supported by all implementations. These controls make messages and media tamper-evident end-to-end.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An integrity protection design confirming TLS deployment on all NGCS/ESInet protocol exchanges with SHA-256, and network-wide support for SHA-256.
- Cipher/algorithm policy and configuration artifacts proving acceptance of SHA-256 and procedures to prevent/detect downgrades.
- Verification & monitoring: evidence that interfaces negotiate required integrity algorithms; ongoing checks to prevent regression.
- Exception handling for legacy interoperability (where deployed), with compensating controls and a timeline to reach full SHA-256 compliance.

4.5.1. JSON Web Signatures (JWS)

The contractor must implement JWS exactly as specified in the NENA i3 Standard (NENA-STA-010.3 §5.10), including, but not limited to, serialization, algorithm, discovery, certificate/chain handling, and Logging Service provisions defined therein. This RFP does not restate i3's normative details; Respondents must conform to i3 requirements as currently defined.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A statement of conformance to JWS requirements of NENA-STA-010.3 §5.10, plus a clause-by-clause matrix mapping the implementation to each i3 requirement.
- Operational policies reflecting i3 requirements and certificate/chain handling with long-term stability where applicable.
- Test/validation evidence showing interoperability and conformance with i3 JWS processing & verification across relevant services.

4.6. Information Privacy

All NG911 protocol operations must be privacy-protected in transit with TLS, and confidential data must be encrypted at rest, in conformance with the NENA i3 Standard and NG-SEC (NENA-STA-010.3 §5.8 & NENA-STA-040.2 §6.22). Implementations must support AES-256 (or stronger equivalent). Algorithms and key lengths must be chosen to protect data for the full retention period. Encryption keys must never be stored in plaintext; with access following a documented management policy – including strong passwords and multifactor authentication required for access. Alternative algorithms are acceptable only if cryptographically equivalent to, or stronger than, AES-256 with end-to-end interoperability support. The contractor should prepare for the ability to upgrade or replace encryption algorithms and parameters to ensure continued conformance with future updates to the NENA i3 and NG-SEC Standards.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A statement of conformance to NENA i3 and NG-SEC privacy & encryption requirements (NENA-STA-010.3 §5.8 & NENA-STA-040.2 §6.22).
- An architecture/configuration overview showing TLS everywhere in transit and encryption at rest for stored confidential data, with cipher/algorithm policies and downgrade protections.
- A cryptographic longevity rationale demonstrating algorithms and key lengths cover the full data lifecycle.

- A key management policy: generation, storage, access control, rotation, backup/restore, and revocation; identification of key custodians and audit practices.
- Operations evidence proving only approved algorithms are enabled and weaker ones disabled; include exception handling and a migration plan for any legacy endpoints.
- If proposing alternates, a strength & interoperability justification confirming parity with AES-256 and end-to-end support across all impacted components.

4.7. Security Assessment and Audit

A cybersecurity assessment/audit verifies conformance/compliance with security requirements, controls, and standards. At a minimum, assessments/audits shall apply the impact categories (low, moderate, high) and security objectives (confidentiality, integrity, availability) defined in NIST FIPS 199 when assessing findings, and use those categories and objectives – together with vulnerability and threat information – to determine risk and remediation priority.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An audit methodology that applies NIST FIPS 199 impact categories and security objectives and explains how impact × likelihood (or equivalent) drives risk ratings and prioritization.
- The proposed audit scope and cadence – initial baseline and periodic re-evaluation – including coverage of ESInet segments, NGCS components, PSAP-facing interfaces, and policy/procedure controls.
- A findings lifecycle including severity assignment using FIPS 199 impacts, remediation due dates, owner assignment, tracking to closure, and verification of issue remediation.
- Integration points with the Risk Management program and with continuous monitoring for follow-up testing of high-severity items.

4.7.1. Assessment and Audit Documentation

Security requirements and risk considerations must be built into development and delivery. Before deployment, every NG911 resource must complete a documented security assessment verifying conformance/compliance with applicable policies and/or requirements. Related components may be assessed as a group when appropriate. Assessment records must be retained as auditable evidence for future reviews.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A pre-deployment security assessment process covering all components with acceptance criteria, approvers, and required evidence.
- Templates and examples of deliverables (control test results, residual risk statements, exceptions & compensating controls, approval sign-off) mapped back to requirements.
- A documentation retention & evidence management plan supporting internal and third-party audits/assessments.
- Integration points with change management and release processes to ensure no promotion to production without a complete, approved assessment.
- A tracking mechanism linking assessment findings/exceptions to remediation or formal risk acceptance and verification of closure.

4.8. Security Monitoring, Detection, and Alerting

4.8.1. Security Event Logging and Continuous Monitoring

Security event logging is essential for early detection, scoping, and investigation of cybersecurity incidents. Logging should be centralized and standardized, tuned to capture only what is necessary, and informed by a baseline of "normal" activity so anomalies can be detected. While "Security Event Logging" objects for the NG911 Logging Service are not yet defined, the contractor's proposed solution must be ready to adopt them when published and leverage current standardized log retrieval functions.

(section continues next page)

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Time synchronization controls proving all logging applications and device clocks align to the time server requirements from NENA-STA-040.2 §5.6.1, enabling cross-system correlation.
- A centralized logging architecture (collection, transport, storage) with coverage to trace and correlate events end-to-end across ESInet/NGCS; include any additional logging for administrative accounts.
- A review/monitoring cadence: at minimum weekly human review, plus a plan to reach near real-time visibility via automation (e.g., SIEM).
- Log integrity & access protections: controls preventing deletion/modification, role-based access, retention periods, and storage locations that satisfy retention requirements.
- Tuning & performance practices showing log scopes/levels calibrated for detection without degrading performance; include the method to establish and update behavioral baselines.
- Forward-compatibility commitment to adopt forthcoming NG911 Security Event Logging specifications on release, including mapping/schema updates for integration with the NG911 Logging Service.

4.8.1.1. Time Synchronization

Accurate, consistent time underpins authentication, logging/correlation, troubleshooting, and continuous monitoring across the ESInet & NGCS. All elements must implement NTP (RFC 5905) and synchronize to a common, resilient time source consistent with NENA-STA-010.3 ('Time' §2.2 & 'Time Server' §4.17). The ESInet must provide an authoritative NTP service backed by a hardware clock or synchronized to external sources with sufficient redundancy to maintain local time during isolation. Service accuracy must be $\pm$ 1ms from true time, and the absolute time difference between any two elements within the ESInet/NGCS must be $\leq$ 0.1 second.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Time architecture showing the ESInet NTP service, upstream sources/hardware clocks, and redundancy/backup design.
- Element compliance evidence that all ESInet/NGCS elements support NTP (RFC 5905) and are configured to the designated time sources
- Accuracy & drift SLAs proving $\pm$ 1ms at the ESInet time service, and 0.1 second max element-to-element skew; include monitoring and alerting for out-of-tolerance conditions.
- Isolation resilience procedures to maintain accurate local time if upstream is unreachable.
- Operational controls: change management for time sources, certificate/time coupling checks, log/time baseline verification, and periodic audits of time-sync configuration and performance.

4.8.2. Denial of Service and Telephony Denial of Service (DoS/TDoS)

A DoS/TDoS attack attempts to render resources unavailable by overwhelming capacity or impeding traffic flow. ESInet providers must have plans and procedures to mitigate and manage DoS/TDoS events. An ESInet must be able to withstand the largest feasible Distributed Denial of Service (DDoS) or TDoS attack, which, as of the current version of NENA-STA-010.3, means $\approx \geq$1 Tbps (terabit per second) of mitigation capacity. This can be achieved via a combination of network/BCF bandwidth and mitigation services.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DDoS/TDoS resilience architecture demonstrating $\approx \geq$1 Tbps (terabit per second) effective mitigation capacity across ESInet ingress, BCF/SBC, upstream carriers, and contracted mitigation services (including how capacity is measured and assured).
- Traffic re-route capability design showing how private links and any Internet-based paths can be redirected to a mitigation service during events; include activation triggers, propagation steps, and rollback.
- Plans and procedures to mitigate and manage DoS/TDoS incidents.
- Operational testing evidence of re-route/mitigation cutovers and load exercises, with results demonstrating maintained call delivery and measured restoration times.

- Monitoring & detection of volumetric and signaling-layer abuse with alert thresholds and dashboards spanning network, BCF/SBC, and application layers.
- Configuration governance for temporary blocks/rate limits and rule updates during incidents, including audit trails and post-incident reviews.

4.8.3. Intrusion Detection and Prevention Systems (IDS/IPS)

The contractor must include intrusion detection to identify known threats and suspicious behavior across endpoints and networks, with alerts routed to a central monitoring function. Intrusion prevention adds automated blocking and must be carefully deployed to avoid disrupting 911 call handling; on segments carrying live call media and signaling, IPS should be avoided unless rigorously engineered, tested, and monitored. Controls must be tuned and maintained so detections remain accurate as the environment changes.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Architecture and placement: where IDS is deployed, where IPS (if any) is deployed, and how alerts flow to a central SIEM; include rationale for deployed controls – ensuring no impact to legitimate media/signaling.
- Content currency & tuning: processes to update signature content at least weekly and to review/update anomaly profiles at least annually and upon material changes; including tuning and drift management.
- Monitoring cadence: procedures for at least weekly human reviews, with staffing/tools that achieve daily or near real-time monitoring; escalation paths and on-call coverage.
- Configuration governance: annual configuration reviews, change controls, test/validation before enabling prevention actions, and rollback procedures.
- Quality management: metrics and methods to track and reduce false positives/negatives, periodic effectiveness reviews, and sample investigation records.
- Integration: how IDS/IPS telemetry correlates with firewalls, endpoint security, event logs, and SIEM; storage/retention aligned to logging requirements and protected against tampering.

4.9. Domain Name System (DNS)

DNS is mission-critical for NG911 service reachability and must be engineered and operated to resist tampering and disruption (e.g., spoofing, cache poisoning, DoS on resolvers). The contractor shall implement defense-in-depth protections (DNSSEC validation/signing, logging, cache-locking, response-rate limiting), and align DNS administration with privileged account, patching, and change-management controls/requirements outlined elsewhere in this RFP.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- DNSSEC is enabled on all deployed DNS servers, and clients are configured to request DNSSEC validation.
- DNS logging is enabled on all DNS servers with centralized collection and retention; describe log scopes and how performance impact is managed.
- Cache locking is enabled and set to 100% of TTL on recursive servers.
- Response rate/time limits are configured on name servers to mitigate DoS/TDoS effects.
- Administrative access controls to DNS infrastructure conform to requirements in NENA-STA-040.2 §6.2.1.3 ‘Administrator Accounts’.
- Patch and update compliance for all DNS components conforming to requirements in NENA-STA-040.2 §5.5 ‘Patching and Updating’ including emergency update procedures for critical CVEs.
- Network placement & resilience: DNS architecture diagrams showing internal vs. external roles, inter-site redundancy, diverse upstream resolvers, and protections at network boundaries.
- Monitoring and alerting for DNS health and integrity (e.g., DNSSEC validation failures, abnormal NXDOMAIN spikes, RRL hits).

Remainder of page intentionally blank

5. Reporting Services Requirements

The contractor shall implement end-to-end logging for all call and transaction events across ESInet and NGCS components in RAW format. Logs must include ISO 8601 timestamps with time zone offset, unique correlation IDs, call identifiers, SIP message summaries (headers and SDP), PIDF-LO snapshots (privacy-redacted), routing decisions, ECRF/LVF responses, PSAP handoff timestamps, and error details. Logs shall be tamper-evident through cryptographic hashing or blockchain-like mechanisms and protected against unauthorized access.

The system shall generate CDRs for every emergency call, capturing fields such as calling line identifier, location used for routing, receiving PSAP ID, call start/answer/end timestamps, media types negotiated, disposition codes, and any transfers. CDR format and fields must align with NENA specifications, supporting export in XML/JSON.

Logs and CDRs shall be retained for a minimum of 7 years (or per jurisdictional policy), with secure storage, searchable indexing (e.g., via Elasticsearch), and export in standard formats (CSV, JSON, PDF). Access must be role-based, with audit trails for queries.

The contractor shall provide data to the PSC data analytics platform to allow for pre-built reports on call volume, average answer time, transfer metrics, location validation failures, and outage incidents, along with ad-hoc querying tools.

The system must maintain auditable trails for all configuration changes, GIS updates, and policy modifications, recording user identity, timestamps, before/after values, and rationale.

5.1. Reporting and Data Collection Requirements

The State requires enterprise-wide reporting and data collection capabilities on all aspects of the proposed NG911 system.

This capability must be agnostic to provider, system or technology and must be able to collect reportable data on the operation, configuration, and maintenance of the NG911 system. This includes both the NG911 systemwide/statewide/enterprise wide and local/PSAP specific data collection, logging and reporting necessary for the processing and documentation of 911.

5.2. Logging Service

The State requires that there be a Logging Service conforming to NENA-STA-010.3. The logging service must be capable of logging all `LogEvent`s defined in NENA-STA-010.3, including media, and all Functional Elements provided under the contract must generate such `LogEvent`s and send them to the logging service.

The State desires that the Logging Service be made available to any PSAP that chooses to use it and implements the required i3 logging interfaces.

The Logging Service must support the query, retrieval, and log event replicator mechanisms described in NENA-STA-010.3.

The Logging Service must support `ElementState` and `ServiceState` SUBSCRIBE/NOTIFY per NENA-STA-010. The State must be able to subscribe to ServiceState and receive the standard state changes.

The proposal shall describe the Logging Service in detail.

5.3. i3 Logging and Reporting Requirements

The proposed solution's NG911 logging and reporting system must conform to NENA-SAT-010.3 i3 logging requirements, including functional element logging, data collection, and reporting.

5.4. Functional Element Reporting

All functional elements within the ESInet (e.g., ESRP, ECRF, LVF, LIS, BCF) MUST be capable of reporting their operational status, critical events, alarms, and other relevant data. This reporting is essential for system monitoring, troubleshooting, security analysis, and performance management. Reporting mechanisms shall conform to standard protocols to ensure interoperability with a centralized logging and monitoring infrastructure.

- ESInet to PSAP Call Delivery transactions
- SIP Conference metrics
- PSAP Routing Duration Report
- Concurrent Calls
- BCF Session Reporting
- ESRP Session Reporting
- ESRP Queue State
- ECRF Session Reporting
- LVF Reporting
- LNG Session Reporting

Respondents must describe the proposed enterprise-wide NG911 logging, data collection, and reporting system and the elements provided above.

5.5. Monitoring, Outages, Failover, Trouble Tickets, and Escalation

The State requires that there be a Network Operation Center (NOC) that monitors the ESInet, the NGCS, the gateways, and all the other elements provided under the Contract. Each element must be continuously monitored for correct operation, and any faults must cause alerts to the NOC.

Any element failure must be treated as an outage. Any service failure must be treated as a serious outage. The proposal must include a description of outage classifications with escalation processes and notification processes. A system outage must have an escalation process that escalates to the highest non-executive level within the committed SLA. For example, an outage on a service with a 5-nines (99.999% uptime) SLA must escalate to the highest non-executive level within five (5) minutes of the outage. In this context, non-executive means all the contractor and appropriate subcontractor technical staff is committed at the highest level, but not necessarily senior executives who could monitor, but not actually contribute to problem resolution. A single person must be designated the owner of such an outage, and that owner must be empowered to direct any available resources to assess, diagnose and repair the cause or effect of the outage. The owner of the outage must be reported to the State promptly.

Any outage visible to any PSAP must be reported to that PSAP and to the State. The proposal must include the available notification methods and timing of reports of outage, progress, and restoration.

Any outage which causes an SLA failure for the month in which the outage occurred must be investigated, the root cause(s) must be determined, and corrective actions must be undertaken. The State and affected PSAPs must receive a report with the root causes, corrective actions and with committed dates. Follow-up reports noting progress against the committed dates must be provided quarterly. The State expressly reserves the right to question the root cause determination and, if it determines that the proposed corrective action plan is deficient, the contractor and the State will negotiate in good faith to amend the root cause and form a corrective action plan that is mutually agreeable.

The State requires that the contractor provide a help desk, which may be the NOC or a different group. The help desk must be staffed 24/7/365 by staff qualified to solve the most common issues encountered by PSAPs. The help desk must have a ticketing system that accepts tickets submitted by website or telephone call. The help desk must be the exclusive mechanism used to report problems by PSAPs or State staff. Every problem report must generate a ticket.

For problem reports received by telephone, the call must be answered by a qualified technician within 60 seconds 90% of the time. For website entered tickets, an initial automated email must be generated immediately, and a follow up email or telephone call must be sent within 5 minutes 99% of the time. The technician first encountering a new issue must be able to solve the problem by taking whatever actions are required to close the ticket themselves 50% of the time. This should be included in a monthly report to offer KPIs.

The help desk must take ownership of all reported problems. Sustained effort must be maintained until the problem is solved and the ticket is cleared.

The State requires that the contractor integrate or "bond" the ticketing systems of each supplier or subcontractor which may be engaged by a ticket, so that the help desk is able to have full visibility and follow up as necessary with such suppliers and subcontractors. The help desk must maintain ownership of issues even if suppliers or subcontractors must solve all or part of the reported problems. However, while the help desk must maintain ownership of the issue, it is incumbent upon the contractor to keep the State informed and fully aware of progress during the effort to restore services. The State prefers that the reporting entity be able to converse with the people who can solve the problem, so if a contractor is solving the problem, the State desires the help desk to keep abreast, but not be in the middle of solving the problem.

When sustained outages (more than 15 minutes) occur, the contractor must investigate and initiate workarounds to bring the system back to at least partial operational state. Even if the actual problem source has been found, and repairs underway, workarounds must be devised to ameliorate the problem if the work arounds can be completed faster than the actual problem repair.

5.6. Maintenance and Configuration Reports

Respondents must provide maintenance and configuration reports once a maintenance issue has been completed or an issue requiring maintenance is resolved. This report shall include a description of the event and the corrective or preventative action taken.

- Lists events by date/time range
- Provides drill down to specific events

5.7. Discrepancy Reporting

Errors and discrepancies may occur in any set of data, including databases, configurations, etc. The functional elements and service will support the NENA-STA-010.3 discrepancy report (DR) function. The discrepancy report function is intended to be generated by any entity that is using the data and finds a problem.

- The Discrepancy Reporting web service will be used by a reporting entity to initiate a Discrepancy Report per NENA-STA-010.3.
- Discrepancy Resolution will follow the NENA-STA-010.3 standard to request the resolution to the DR and sends the resolution to the Resolution Uri parameter in the report request.
- Entities will have access to discrepancy status updates.

The Discrepancy Report (DR) function supports a phased response like the following:

- The reporting entity creates the DR and submits it to the responding entity.
- The responding entity acknowledges the DR and provides an estimate of when it will be resolved.
- The reporting entity may request a status update and receive a response.
- The responding entity resolves the DR and reports its resolution to the reporting agency.

All DRs MUST contain common data elements (a prolog) that include:

- Time Stamp of Discrepancy Submittal
- Discrepancy Report ID (a unique value generated by the reporting entity)
- Discrepancy reporting entity FQDN
- Discrepancy reporting agent user ID
- Discrepancy reporting contact info
- Service or Instance in which the discrepancy exists.
- Discrepancy Report type (from the list of DRs in this section)
- Additional notes/comments
- Reporting entity's assessment of severity

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Support for NENA-STA-010.3 DR function generated by data users.
- Discrepancy Reporting web service for initiating a DR.
- Resolution per standard to Resolution URI.
- Access to status updates.
- Phased response (create/submit, acknowledge/estimate, status update, resolve/report).
- Common prolog elements (timestamp, ID, FQDN, user ID, contact, service/instance, type, notes, severity).

5.7.1. Policy and Core Routing

5.7.1.1. Policy Store Discrepancy Report

A client of a Policy Store may report a discrepancy. This type of DR most commonly arises when a Policy Query returns an invalid Policy from the Policy Store. A Policy Owner may retrieve a policy it previously stored to verify the query returns an exact match to the one that was stored; if not, then a DR should be filed against the Policy Store. A policy store may report a discrepancy against itself to raise an issue.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Policy Store DR against Policy Store

5.7.1.2. Policy Discrepancy Report

A Policy Discrepancy Report function will be implemented per NENA-STA-010.3. Any entity (such as an ESRP) using a policy (such as a routing policy) will be able to report a discrepancy against the owner of the policy (e.g., a PSAP or an ESRP).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Policy DR against policy owner (e.g., PSAP/ESRP).

5.7.1.3. Emergency Services Routing Proxy (ESRP) Discrepancy Report

An ESRP Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. A PSAP or other entity will be able to report a discrepancy against an ESRP when a call is received that should not have been routed to the PSAP, or the ESRP has one or more queues whose fullness is a problem, or if the PSAP seems to be receiving fewer calls than would normally be expected. A routing problem may be the result of incorrect data in the ECRF (GIS data). Calls are sent to PSAPs by ESRPs (Emergency Services Routing Proxy), so a PSAP should report a problem to the ESRP. The ESRP, in turn, reports any suspected GIS problems to the ECRF.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 ESRP DR for misrouted calls, queue fullness, low volume; ESRP reports GIS issues to ECRF.

5.7.2. Location and GIS Sources

5.7.2.1. Location Information Server (LIS) Discrepancy Report

The contractor will include a LIS Discrepancy Report function per NENA-STA-010.3. Any client of a LIS will be able to report a discrepancy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 LIS DR for LIS clients.

5.7.2.2. GIS Discrepancy Report

The contractor will include a GIS Discrepancy Report function per NENA-STA-010.3. With this mechanism, the LoST server or other entity will be able to report a discrepancy report against GIS data.

Expected reports include: A gap or overlap discovered when data is coalesced.

- Incorrect information (such as the LoST server to query for information about an area)
- Bad GIS data (such as bad geometry, duplicate attributes, omitted mandatory information, incorrect data type, an address range issue on centerline, a general provisioning failure, or a malformed URI).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 GIS DR for gaps/overlaps, incorrect info, bad data (geometry, attributes, ranges, provisioning, URI).

5.7.2.3. MSAG Conversion Service Discrepancy Report

A MSAG Conversion Service (MCS) Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. An LSRG or other entity will be able to report a discrepancy against the MSAG Conversion Service (MCS) when a conversion fails, but the querier believes it should have succeeded. A DR may also be filed when the conversion succeeded but the returned location from the MCS is not MSAG-valid or LVF-valid. Both these errors can occur in either direction (PIDF-LO to MSAG or MSAG to PIDF-LO).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 MCS DR for failed conversions or invalid returned locations (PIDF-LO/MSAG bidirectional).

5.7.2.4. LoST Discrepancy Report

The contractor will include a mechanism for any client of an LVF/ECRF/LoST server to report a discrepancy per NENA-STA-010.3.

The expected reports are:

- The LoST server reports a location as invalid when the client believes it is valid.
- A LIS MAY report a discrepancy against an LVF (as well as against an Originating Service Provider) if a civic address provisioned by an Originating Service Provider for a fixed device is reported invalid by an LVF.
- The LoST server returned an incorrect route in a `findServiceResponse`.
- The LoST server returned an incorrect error or warning regarding the location.
- The `getServiceBoundaryResponse` is incorrect.
- The `listServicesResponse` is incorrect.
- The `listServicesByLocationResponse` is incorrect.

Other discrepancies may be reported but are expected to be less common. These include:

- A client received an address reported as valid that it considers invalid.
- Multiple mappings were returned when only one was expected.
- Incorrect service number(s) returned.
- Expired data returned.
- An incorrect <Uri> element was returned.

A DR against a LoST server must also support the ability of the LoST server to report a discrepancy against the GIS data.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Mechanism for LVF/ECRF/LoST client to report discrepancies (invalid location, incorrect route/error/warning, incorrect responses).
- Support for LIS reports against LVF/OSP.
- LoST server reports against GIS data.

5.7.3. Signaling and Edge

5.7.3.1. SIP Discrepancy Report

The contractor will have a NENA-STA-010.3 SIP Discrepancy Report function. Entities that encounter an error communicating with another entity via SIP (such as a PSAP) will be able to report a discrepancy.

The expected reports are:

- An initial INVITE request failed.
- A MESSAGE request failed.
- An OPTIONS request failed.
- A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed.
- Required media stream (audio, text, video) failed to be accepted.
- Media problems during a dialog.
- Signaling failure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 SIP DR for comm errors (failed requests, media stream failures, media problems, signaling failure).

5.7.3.2. Border Control Function (BCF) Discrepancy Report

The contractor will have the BCF Discrepancy Report function as defined in NENA-STA-010.3. This function allows for an entity routing traffic through (to or from) a BCF to report a discrepancy.

The expected reports are:

- Traffic incorrectly blocked before a dialog has been established (e.g., an INVITE, MESSAGE, or OPTIONS request, or response blocked).
- Traffic incorrectly blocked during a dialog.
- SIP signaling is inappropriately modified or dropped.
- Session Description Protocol (SDP) incorrectly regenerated during B2BUA/media anchoring.
- Media relayed with loss.
- Traffic permitted that should have been blocked because a designated bad actor generated it.
- Traffic permitted that should have been blocked for some other reason.
- QoS inconsistency.
- Invalid or improper Call Detail Recording.
- TTY to RTT transcoding errors.
- Firewall (non-SIP) errors.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 BCF DR for traffic routing issues (blocked/modified/dropped traffic, SDP regeneration, media loss, permitted bad actor traffic, QoS inconsistency, invalid CDR, TTY-RTT errors, firewall errors).

5.7.4. Network and Infrastructure

5.7.4.1. Network Discrepancy Report

A Network Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. Any entity will be able to report a general networking discrepancy.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 general networking DR.

5.7.5. Security and Trust

5.7.5.1. Permissions/Security/Authentication Discrepancy Report

The contractor will deliver a Permissions/Security/Authentication Discrepancy Report function as defined by NENA-STA-010.3. Entities that identify a security issue or a permissions or authentication error that is believed to be incorrect, will be capable of reporting a discrepancy using the DR interface of the entity or element believed to be responsible for the discrepancy.

The expected reports are:

- Unable to authenticate.
- Unable to SUBSCRIBE to an event package.
- Permitted to SUBSCRIBE to an event package when it should have been denied.
- Unable to read a resource.
- Unable to write/modify a resource.
- Unable to delete a resource.
- Able to read a resource when it should have been denied.
- Able to write/modify a resource when it should have been denied.
- Able to delete a resource when it should have been denied.
- Unable to establish secure communication (e.g., TLS certificate is invalid or TLS failure).
- Unable to verify digital signature of a resource (e.g., a routing policy signature verification failed, or the certificate chain is invalid or contains an untrusted authority).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Reports for security/permissions/auth errors (unable to auth/subscribe/read/write/delete, able when denied, TLS/certificate/signature failures).

5.7.5.2. Log Signature/Certificate Discrepancy Report

A Log Signature/Certificate Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. When an entity (e.g., a Logging Service or another entity) that verifies LogEvent signatures is unable to obtain a certificate, encounters an invalid certificate or thumbprint, or the signature verification fails, it will be able to report the discrepancy to the entity that generated the LogEvent.

The expected cases for this Discrepancy Report are:

- The certificate cannot be obtained (no “x5c” nor “x5u” field provided).
- The “x5u” field cannot be resolved or does not resolve to a valid certificate.
- The “x5u” field is present but the “x5t#256” field is missing, or the thumbprint specified does not match the certificate obtained from the “x5u” field.
- The signature of a LogEvent does not verify.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 report for certificate/signature issues (unobtainable/invalid cert, mismatched thumbprint, failed verification).

5.7.6. Data and Logging

5.7.6.1. Logging Service Discrepancy Report

The contractor will have a Session Recording Client (SRC) or any entity generating logging events to, or retrieving logging records from, a Logging Service that may report a discrepancy.

The expected reports are:

- An SRC encountered an error inviting the SRS.
- LogEvent returned an error when it should not have.
- RetrieveLogEvent returned an error when it should not have.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SRC/entity reports for errors in inviting SRS, LogEvent, or RetrieveLogEvent.

5.7.6.2. ADR/IS-ADR Discrepancy Report

An ADR/IS-ADR Discrepancy Report mechanism per NENA-STA-010.3 will be provided. A PSAP, ESRP, ECRF, or other entity or function will be able to report a discrepancy against an ADR or IS ADR.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 ADR/IS-ADR DR by PSAP/ESRP/ECRF/etc.

5.7.7. PSAP Operations and Treatments

5.7.7.1. PSAP Call Taker Discrepancy Report

The contractor will include the ability for a PSAP, downstream agency, or other entity to report a discrepancy against a PSAP Call Taker when a call is received that should not have been transferred to the reporting entity.

The resolution parameter in a DiscrepancyResolution report per NENA-STA-010.3 requires one of the following tokens:

- CallTakerAdvised (the call taker who transferred the call has been advised that the transfer was in error)
- TransferCorrect (the transfer was correct)
- NoDiscrepancy
- OtherResponse

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Reports against PSAP Call Taker for erroneous transfers.
- Resolution tokens (CallTakerAdvised, TransferCorrect, NoDiscrepancy, OtherResponse).

5.7.7.2. Call Transfer Failure Discrepancy Report

A Call Transfer Failure Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. A PSAP, LSRG, or other entity will be able to report a discrepancy against a transfer entity when a transfer fails. The notification should be made to both the entity originating the transfer and the entity receiving the transfer.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 mechanism for transfer failures, notified to originating/receiving entities.

5.7.7.3. Interactive Media Response (IMR) Discrepancy Report

An Interactive Media Response (IMR) Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. Any entity aware of a discrepancy at an Interactive Media Response (IMR) will be able to report a discrepancy at it.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 IMR DR.

5.7.8. External Providers

5.7.8.1. Originating Service Provider Discrepancy Report

A mechanism for Originating Service Providers to file Discrepancy Reports will follow NENA-STA-010.3. The service allows an entity to create a discrepancy against an Originating Service Provider when a location provided by the Originating Service Provider fails validation.

- An ECRF or ESRP or PRF or PSAP may report a discrepancy when a default location is used for routing because the location is missing or not usable.
- An LNG or other entity may report a call received without ANI.
- An LNG or ESRP or other entity may report that a badly formed PIDF-LO was received, or a location query timed out without receiving a PIDF-LO.
- An LSRG or other entity may report that a call was dropped or terminated without appropriate signaling.
- A PSAP may report a discrepancy when a civic location received with a fixed (wireline) call is incorrect.
- A BCF, ESRP, PSAP, or other entity may report an incorrectly formed call (e.g., a SIP INVITE that is badly formed, lacks certain header fields or body parts, etc.).
- A BCF, ESRP, PSAP, or other entity, may report that an unusually large call volume (which might suggest a DoS or other attack) or an unusually low call volume is being generated by the Originating Service Provider.
- An Originating Service Provider may report a discrepancy against itself to raise an issue to be addressed.
- An entity may report a discrepancy when an Additional Data Reference included in the call is invalid.
- An entity may report a discrepancy when an Additional Data value is invalid.
- The Secure Telephone Identity-Verification Service (STIVS) FE may report a Secure Telephone Identity verification failure to an Originating Network.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Mechanism per NENA-STA-010.3 for OSP DRs (invalid/missing location, no ANI, bad PIDF-LO/query timeout, dropped call, incorrect civic, badly formed INVITE, unusual volume, invalid Additional Data, STIVS verification failure).
- Self-reports by OSP.

5.7.9. Test and Tools

5.7.9.1. Test Call Generator Discrepancy Report

A Test Call Generator Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. When a Test Call Generator encounters errors initiating or processing a test call, it reports the discrepancy to the PSAP that should have received the test call.

The expected cases for this Discrepancy Report are:

- An initial INVITE request failed.
- A MESSAGE request failed.
- An OPTIONS request failed.
- A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed.
- Loopback media stream (audio, text, video) failed to be accepted.
- Loopback media problems during the test dialog.
- Signaling failure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Test Call Generator DR to PSAP for errors (failed requests, loopback failures, media/signaling issues).

6. Installation Requirements

Respondents are required to assume the primary project management and installation management role for their NG911 system. The State will aid and coordinate support for some aspects of the installation but will be looking for the Respondent (Contractor) to provide all installation services.

Installation as defined in this RFP includes:

- Coordination with PSAPs
- System and service migration (i.e., logging, recording, CAD)
- Coordination with OSPs
    - Ingress
    - Core
    - Egress
- Coordination with current 911 system service provider
    - Ingress
    - Core
    - Egress
- Traffic migration
- Data migration
- Staging
- Testing
- Pre-cutover
- Cutover planning
- Training

The Respondent must, at a minimum, provide installation, maintenance, and support services for the duration of the contract period. Customer service support functions are identified below (§E-9, et seq.) and must be included in the Proposal to ensure that the network is fully supported.

6.1. Installation Services

The Contractor is responsible for the installation of all requirements listed in the RFS and attachments and any other functional elements such as power and UPS as necessary to implement their NG911 solution. Devices that are installed at a PSAP may require analysis of the power and backup power supply at that PSAP. In some cases, the contractor may need to remediate issues to ensure their device has the resources needed. The State may aid coordination support for some aspects (such as approvals and scheduling) of the installation but is relying upon the Contractor to perform all installation services.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Methodology for installation of all NG911 system components and explain the approach to completing installation of the delivery of NG911 traffic. The methodology must include coordination with OSPs, PSAPs and other potential networks that can enhance the delivery of 911 traffic across the system.
- Coordination methodology to interconnect with all current telecommunication companies that are responsible for 911 call delivery and explain how these providers are accounted for during implementation.
- Plan to coordinate with all current 911 system service providers.
- Installation services to be provided and outline the roles and responsibilities of the Contractor and Subcontractor(s) during installation. Installation tasks as defined include, but may not be limited to:
    - Coordination with PSAPs
    - System and service migration (i.e., logging, recording, CAD)
    - UPS integration to support a minimum 3-hour backup validated with an MTTR / MTBF calcuation
    - Coordination with OSPs
    - Coordination with current 911 system service provider
- Traffic migration
- Data migration

- Staging
- Acceptance testing
- Cutover planning
- Training

6.2. Wiring and Cabling

All interface connections and visible cables must use standard EIA connectors secured by wall plates where exposed.

All cables must be clearly marked and/or numbered in a manner that reflects a unique identifier of the cable at both ends.

Any cables used must be plenum rated where required by local building or fire codes.

Respondents must ensure that all equipment is connected to emergency AC power and is configured to be supported by a UPS.

Cabling, communications outlets, power wiring, system grounding, conduit facilities, and equipment rooms must be installed in accordance with national standards and applicable local codes.

The minimum standards used in the installations shall include, but are not limited to, the following:

- ANSI/TIA/EIA-568 – Commercial Building Telecommunications Wiring Standard
- ANSI/TIA/EIA-569 – Commercial Building Standard for Telecommunications Pathways and Spaces
- ANSI/TIA/EIA-606 – Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
- ANSI/TIA/EIA-607 – Commercial Building Grounding and Bonding Requirements for Telecommunications
- Building Industry Consulting Service International, Telecommunications Distribution Methods Manual
- National Electrical Code (NFPA-70)
- FCC Rules and Regulations, Parts 68 and 15

6.3. Grounding

The proposed system must provide surge and lightning protection for all connections to AC power and is required to meet the R-56 standard.

All hardware and peripheral devices must be mechanically and electrically grounded to prevent both user hazard and loss of data or hardware integrity due to external electrical impulse.

Respondents must ground all equipment in compliance with manufacturer recommendations and applicable standards.

Respondents must furnish and install the required grounding and bonding conductors where necessary and complete the connections to the grounding system at all sites.

Remainder of page intentionally blank

7. Training

The Respondent shall work cooperatively with the State and designated staff to deliver training for the proposed solution. Training shall be ongoing throughout the term of the contract, with the ability to provide on-demand sessions at the State's request. The Respondent must include a description and supporting documentation for all requirements in this section.

7.1. Audiences and Scope

PSAP Operations:

- Network status reports
- Help desk usage and processes
- Text-to-911 operations
- Text- from-911 operations
- Trouble Ticketing

State-Level Operations:

- Network status reports
- Help desk processes
- Trouble ticketing
- Root-cause analysis and review

7.2. Training Elements

The Respondent shall develop and deliver training to meet the following minimum requirements:

- Login and logout procedures
- Password reset
- Equipment problem reporting
- Call transfer functionality
- Call conferencing functionality
- Discrepancy reporting
- Foreign language interpretation process
- Rebid/refresh of call information
- Instant recorder/playback
- Text-to-911
- Text-from-911
- Other solution features not otherwise listed

7.3. Technical Assistance

Upon request by the State, the Contractor shall provide technical assistance to PSAP personnel during training and testing.

7.4. Schedule and Locations

No later than fourteen (14) calendar days before each PSAP cutover, train all PSAP personnel (including State and administrative personnel assigned to the PSAP) on the proper operation of all Contractor-supplied software and equipment. To maintain the deployment schedule and accommodate call-taker travel, the Contractor shall establish temporary training site(s) in Nebraska as needed and provide weekend and evening sessions when required.

7.5. Training Materials

Provide all training materials and a Train-the-Trainer (TtT) curriculum for State approval. Maintain up-to-date training materials at the State for the duration of the contract.

7.6. Post-Deployment Training and Costs (Proposal Requirement)

The Respondent shall, as part of their response:

- Provide a proposed cost for post-deployment training for up to fourteen (14) students per class
- Provide a proposed cost for the post-deployment TtT course, including the maximum class size.

7.7. Comprehension, Testing, and Certification

Apply testing at intervals during initial and ongoing training and provide the State a final evaluation of each student's knowledge upon completion. Instructional methodologies shall include lectures, group discussions, audiovisual methods, and role-playing. Testing methodologies shall include written exams, oral exams, hands-on testing, and end-of-course certification.

7.8. Training Plan and Samples (Proposal Requirement)

The Respondent shall, as part of their response:

- Provide a proposed training plan and sample documentation and/or materials covering the topics and audiences listed in §E-8.1 and §E-8.2, above.

Remainder of page intentionally blank

8. Operations and Service Management Requirements

The Contractor shall manage all service support for the NG911 system, including integration of service and support for all partners and Subcontractors delivering components to the State.

Service levels and escalation: The Contractor shall commit to 99.999% availability for core voice paths, MTTR < 2 hours for Priority 1 incidents, and defined response times (for example, 15-minute acknowledgment). Include documented escalation paths, root-cause analysis reports, and penalty provisions for SLA breaches.

Operations enablement:
Provide comprehensive training curricula (in-person and virtual), role-based certifications, and operational runbooks for common scenarios such as failover and GIS updates. Supply full technical documentation that uses NENA functional-element nomenclature and is tailored to PSAP operators, network administrators, and GIS staff.

Change management:
Establish documented change-control protocols, including scheduled maintenance windows during off-peak hours, rollback procedures, impact assessments, and at least 30 days' advance notice for changes that affect routing, GIS, or call handling.

Standards conformance and interoperability:
Demonstrate conformance to NENA i3 and NGCS standards through self-attestation and participation in multi-vendor interoperability events (for example, NENA ICE). Test plans shall include NENA-defined sequences, and the system shall interoperate with third-party equipment (for example, CHE from different vendors).

Testing program:
Execute a phased testing program covering unit tests, component integration, system integration, failover simulations, performance, and load testing (including 200% of peak capacity), and security validations using NENA test cases. Success criteria shall include 100% pass rates for critical flows.

Product documentation:
Provide thorough user manuals, API specifications (in OpenAPI format), and release notes, along with the training programs noted above, aligned with NENA terminology.

8.1. Service Management Framework

8.1.1. Service Management Plan

Oversight of the NG911 system and services post implementation/transition is required. The preferred best practice is to utilize Information Technology Infrastructure Library (ITIL) as a guideline for how NG911 services are designed, implemented, managed, maintained, and improved within the term of the contract.

ITIL integrates five stages of service delivery into a comprehensive methodology for managing the lifecycle of services.

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Within these stages are specific areas relating to Information Technology Service Management.

At a high level, these areas reference how a service maintains availability, capability, capacity, security, manageability, and operability. Respondents must describe their approach to service management for the operation of the NG911 system. The NG911 service management approach shall incorporate components of ITIL or follow industry best practices for IT service management.

Respondents must provide a narrative of how their proposed service management approach is integrated into their project management activities. Respondents must discuss their ability to maintain consistent performance and the service levels of the network

Respondents must discuss their ability to maintain consistent performance and the service levels of the network to support the following framework:

- Determination of the single point of contact
- Management of subcontracted support components
- Support personnel required and identification of Key Personnel
- Underpinning contract management
- Third-party support contracts
- Pre-emptive support
- Equipment refreshes
- Preventative maintenance
- Bug fixes
- Patching and upgrades
- Warranty
- Out of warranty items
- Service Level Agreements

8.1.2. Service Level Agreement (SLA)

The NG911 system will utilize the requirements outlined in this RFP to negotiate a Service Level Agreement (SLA) with the selected vendor. In preparation all Respondents must provide a description of their SLA performance measures and identify how the thresholds that are not met are recovered.

The Respondent shall negotiate a comprehensive Service Level Agreement (SLA) framework that defines specific, measurable, achievable, relevant, and time-bound (SMART) metrics for the performance, availability, and reliability of the ESInet and all its functional elements. This framework must detail the processes for monitoring, reporting, and reviewing SLA compliance. The approach should align with industry best practices for IT service management and project management to ensure consistent quality and continual improvement.

The State expects the Respondent to provide a description of how each of these components are met within their SLA.

The State recognizes the following categories as expectations for their SLA.

Critical – Network Outage

- 1st Level Support – Immediate
- Continuous problem resolution/workaround effort
- 2nd Level Support – within 15 minutes
- 3rd Level Support – within 30 minutes or upon Customer request.

Major – Service effecting

- 1st Level Support – Within 5 minutes
- 2nd Level Support – Within 30 minutes
- 3rd Level Support – Within 2 Hours or upon Customer request.

Minor – Non-service effecting

- 1st Level Support – Within 30 minutes
- 2nd Level Support – Within 2 Hours
- 3rd Level Support - Within 1 business day or upon Customer request.

The Respondent must provide a description and/or documentation that supports the requirements in this section.

8.1.3. Compliance and Risk Management

The State requires the contractor to run a documented risk management program for all NGCS components and the ESInet. The program must identify assets, threats, and vulnerabilities; rate and rank risks by **likelihood** and **impact** on **call delivery, location accuracy, security, availability, latency, and resilience**; and select a treatment (reduce, avoid, transfer, or accept). Any non-compliance with security requirements, standards, procedures, or practices must be documented and submitted to the State for written approval, including criticality analysis and a corrective action and/or risk acceptance path.

Each risk under the contractor's control or those outside of the contractor's span of control that will negatively impact the ESInet or NGCS must be recorded on a risk acceptance form and signed by a member of the contractor's senior leadership with the authority – and financial/legal responsibility – to accept that risk for the NGCS/ESInet scope.

All risks must be reassessed at least annually, and high/critical risks at least monthly. The method may use qualitative (very low ↔ very high) or numeric scales but must address both likelihood and impact.

Third-party risks (carriers, cloud providers, data suppliers, managed services, subcontractors) must be tracked and visible even when control is limited. Where a third-party risk could affect service to the State, the contractor must implement compensating controls and define escalation tied to SLA/SLOs (e.g., uptime, MTTR).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A documented Risk Management methodology covering asset identification, threat identification, vulnerability assessment, risk assessment and prioritization, and risk treatment selection (reduction, avoidance, transfer, acceptance). Include working definitions of threat, vulnerability, and risk, and show how business impact is mapped to NGCS/ESInet outcomes (call completion, routing location, latency, availability).
- A risk register template and sample entries showing fields for asset, threat, vulnerability, likelihood, impact, inherent and residual risk, selected treatment, owner, due dates, status, and verification of closure. Include examples for both NGCS applications and ESInet network elements.
- A risk acceptance form/template and completed examples that quantify or qualify likelihood and impact, reference the related non-compliance (if applicable), and record a senior leadership signature with authority to accept risk on behalf of the contractor for the NGCS/ESInet scope.
- Review cadence and triggers, showing at least annual reassessment of all risks and monthly reassessment of critical/high risks; include procedures to re-evaluate on material changes (e.g., carrier migrations, cloud region moves, software upgrades, configuration changes, new interconnections) or emerging threats.
- A third-party risk approach, including how contractor/subcontractor/carrier/cloud risks are tracked (e.g., supplier registers, attestations), how visibility is maintained when direct control is limited, required compensating controls, and escalation timelines aligned to SLAs/SLOs.
- Non-compliance linkage, showing how unresolved non-compliance (policy gaps, audit findings, penetration test results, vulnerability scans) is converted to corrective action or formal risk acceptance within the same process, with State notification/approval where required.

8.1.4. Monthly Project Review and Compliance

The contractor shall meet with the PSC and any of the PSC designated resources at a minimum of monthly throughout the contract period. The frequency of these meetings may be adjusted by the PSC at any time based upon the project lifecycle. Additionally, the agenda of the meeting may be modified based upon any pressing issues that need attention.

The contractor is responsible for providing a report to the State each month that details:

- **Monthly Project review and timeline updates** to document a regular consistent path toward full implementation of the items within the contract
- **Regular Process Audits** to validate adherence to procedures, assess process maturity, and document any corrective actions.

- **Monthly System status and performance** summarizing the performance of the system with details such as utilization, packet success rate, call success rate, traffic path utilization, call transfer updates, database updates, and contract compliance
- **Monthly Service Level Agreement / and Service Level Objective** status vs the Key Performance Indicators in the SLA.
- **Monthly Risk Management Reports** providing updates to the risk register, risk response (impact and priority) to proactively communicate potential triggers that can cause the system harm.
- **Monthly Change Management Reports** summarizing all changes (planned, emergency, completed, deferred, and failed).
    - **Comprehensive Audit Trails** for all changes, retained for a minimum of three (3) years and available to the State upon request.

The contractors monthly project review process shall:

- Ensure the State is regularly informed of any roadblock or constraint in a proactive manner
- Address issues that arise before they become a barrier
- Regularly assess compliance with applicable **NENA i3** standards.
- Support compliance with **47 CFR Part 9, CJIS Security Policy, HIPAA** (where applicable), and State-level cybersecurity directives.
- Align with **PMI PMBOK** integrated principles.
- Conform to **ITIL v4** practices.
- Ensure traceability of all activities and all provisions of the contract to maintain expectations of the State of Nebraska.

8.2. Continuity and Resilience

8.2.1. Availability

The entire IP path, and call-related services, data transactions, and associated services will be available 99.999% of the time, end to end, with the appropriate caveat for PSAPs that do not have the necessary redundancy to maintain 99.999%. Provisioning services not related to call time, such as provisioning the location database in the LNG by legacy OSPs, will be available 99.9% of the time.

Availability is defined as:

MTBF / (MTBF+MTTR)

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 99.999% availability for IP path/call services/data transactions end-to-end (with caveat for non-redundant PSAPs).
- 99.9% for non-call provisioning

8.2.2. Continuity of Operations Plan (COOP)

The Continuity of Operations plan will include measures to account for common cyber security threats and “sunny day” outage vulnerabilities that could affect the normal operation of the NG911 system and cause an outage.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Measures for cyber threats/"sunny day" outages causing system disruptions.

8.2.3. Disaster Recovery (DR)

The Disaster Recovery Plan will include the procedures for:

- Activation procedures
- Recovery team identification
- Roles and responsibilities

- Recovery strategies and response
- Recovery management procedures
- Recovery cost procedures
- Recovery resources
- Recovery communications
- Stakeholder management
- Subcontractor, Supplier, Partner communication, and coordination

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- DR Plan with activation procedures, team ID/roles/responsibilities, strategies/response, management/cost/resources/communications, stakeholder/subcontractor coordination.

8.3. Operations Centers and Support

8.3.1. Network Operations Center (NOC)

The NOC must operate on a 24×7×365 basis for the duration of the contract. In addition, the NOC will include the capability to perform remote maintenance and restoration of alarms, as necessary.

The NOC will be the single point that performs continuous monitoring, maintenance, and network support services of the NG911 System. The NOC will interface with the help desk and the PSAPs or designated staff. The NOC will be staffed with appropriate technical resources to aid troubleshooting, diagnosis and recovery from issues related to the operation of the NG911 system.

The NOC will perform monitoring of the entire ESInet, all connections and functional components used in the routing of 911 calls. The NOC will be equipped with a Network Management System (NMS) that monitors the performance of the network and infrastructure of the NG911 system.

- The NMS will continuously monitor the performance and availability of all devices.
- The NMS will monitor network performance, including throughput, latency, jitter, packet loss, and other parameters deemed necessary by the State.
- The NMS will monitor the network for network intrusion attempts or security breaches and be capable of issuing security alerts when an event is recognized.
- The NMS will create alarms based on thresholds and parameters and distribute alarm notifications appropriately.
- The NMS will monitor the environment at all data centers or points of presence where critical network components are housed to ensure functionality.
- The NMS will monitor ancillary network components such as power utilization and backup power systems.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24×7×365 NOC with remote maintenance/restoration.
- Single point for monitoring/maintenance/support.
- Interface with help desk/PSAPs.
- Staffed for troubleshooting/recovery.
- Monitoring of ESInet/connections/functional components.
- NMS for device performance/availability, network params (throughput/latency/jitter/packet loss), intrusion/breaches with alerts, threshold-based alarms/notifications, data center environment, power utilization/backup.

8.3.2. Security Operations Center (SOC)

The proposed solution requires the services of a Security Operations Center (SOC). The SOC (Security Operations Center) may be combined with the NOC and shares the overall requirements. The SOC must provide support for the following items:

- 24×7×365 operation.
- Capability to perform remote maintenance and restoration of security events.
- Single point that performs continuous monitoring, maintenance, and network support services of the NG911 System and identifies security faults.
- Interfaces with the help desk and the PSAPs or designated staff.
- Staffed with appropriate technical resources to aid troubleshooting, diagnosis, and recovery from security issues.
- Perform security monitoring of the entire NG911 system, all connections and functional components used in the routing of 911 calls.
- Security compliance testing, penetration testing, vulnerability testing, etc.
- Collection and monitoring security logs, and assist with incident response
- Operational security administration such as identity & access management, key management, firewall administration, etc.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24×7×365 SOC (possibly combined with NOC) with remote maintenance/restoration of security events.
- Single point for monitoring/maintenance/support identifying security faults.
- Interface with help desk/PSAPs.
- Staffed for security troubleshooting/recovery.
- Security monitoring of system/connections/components.

8.3.3. Help Desk

A help desk will be included with the NG911 system. The help desk(s) will operate on a 24×7×365 basis and be adequately staffed by resources who are trained and qualified in help desk and customer support services.

The help desk will serve as a single point of contact for all NG911 system and service matters, including without limitation, the NG911 system, all components of the NG911 system, and any additional system service providers delivering services or components for the NG911 ecosystem.

Only a fully staffed help desk will be considered. The help desk must not use an automated attendant or other automated means of answering a call.

The help desk must be accessible via various methods including voice, text, email, and other means as deemed appropriate or as directed by the State.

The help desk will have the ability to communicate directly and immediately with maintenance and support services for the NG911 system and all components of the system, including, without limitation, network troubles. This includes partner providers who are performing or supplying services within the system.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24×7×365 staffed help desk trained in support.
- Single point for all system matters/components/providers.
- No automated attendant.
- Accessible via voice/text/email/etc.
- Direct/immediate communications with maintenance/support including network troubles/partners.

8.3.3.1. Trouble Handling and Ticketing Requirements

Trouble handling, and trouble ticket tracking services will be required for the successful operation of the NG911 system and services.

To ensure that all trouble tickets are resolved in a timely manner, The contractor will develop and maintain an escalation guideline document that describes the escalation procedure.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Trouble handling/tracking.
- Escalation guideline document/procedure.

8.3.3.2. Monitoring of Applications and Equipment

Proactive monitoring of all NG911 system components for operation, performance, and fault conditions will be provided.

The contractor will ensure that all alarms including environmental status alarms are received and monitored in a Network Operations Center (NOC).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Proactive monitoring of components for operation/performance/faults.
- Receipt/monitoring of alarms including environmental in NOC.

8.3.3.3. Root Cause Analysis

The contractor is required to provide a complete Root Cause Analysis (RCA) for any trouble with the system. The RCA process will follow a process like the following:

- Following any critical event or major outage, the State/designated staff must receive a root cause analysis within five (5) business days.
- Immediately after a trouble has been identified the contractor will begin documenting the information as they complete the RCA. This documentation will be made available to the State via a shared online platform that will allow for constant tracking by the State as more information becomes available.
- The RCA format will include dates, times, and discoveries by the contractor as they investigate the trouble.
- Once the investigation has concluded the RCA must be submitted to the State for acceptance and approval that the trouble has been resolved.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- RCA for troubles (within 5 business days for critical/outages).
- Immediate documentation shared online.
- Format with dates/times/discoveries.
- Final submission for State approval.

8.3.4. Customer Support Services

The Respondent must provide a description and/or documentation that supports the requirements in this section, including SLA management (performance/monitoring/delivery/reporting/review); event/incident management; diagnostics/reporting; problem resolution/trouble handling; network fault monitoring; request fulfillment; access management; remote diagnostics; environmental requirements; capacity/change/configuration/transition management; training; commercial availability; all tied to SLOs for SLA measurement.

The contractor is required to provide monthly updates to the PSC regarding the performance of the system in the form of a Monthly Performance Review which is used to measure adherence to the contract elements, the performance measures, and Key Performance Indicators (KPIs). The KPIs are directly tied to the SLA.

Anticipated support services include:

- Service Level Agreement (SLA) management
  - Performance measurement and monitoring
  - Guaranteed delivery
  - SLA reporting and review
- Event management
- Incident management
- Diagnostics and reporting
- Problem resolution/trouble handling
- Network fault monitoring
- Request fulfillment
- Access management
- Remote diagnostics
- Environmental requirements
- Capacity management
- Change management
- Configuration management
- Transition management
- Training arrangements
- Commercial availability

Each of the items listed above are tied to Service Level Objectives (SLO) that the State measures against the Service Level Agreement (SLA).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SLA management (performance/monitoring/delivery/reporting/review) on a monthly basis to the PSC.
- Event/incident management.
- Diagnostics/reporting.
- Problem resolution/trouble handling.
- Network fault monitoring.
- Request fulfillment.
- Access management.
- Remote diagnostics.
- Environmental requirements.
- Capacity/change/configuration/transition management; training.
- Commercial availability.
- All tied to SLOs for SLA measurement.

8.4. Monitoring and Event Management

8.4.1. Alarm Categories

Alarms by event types depending on the criticality of the event (i.e., critical, major, etc.) will be provided. Dynamic configuration of notification thresholds will be utilized to allow new alarm categories to be defined, as necessary.

The system will have automatic notification of the NOC when alarm conditions are detected. Different notification and escalation procedures may apply depending on the alarm category.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Alarms by criticality (critical/major/etc.).

- Dynamic notification thresholds for new categories; automatic NOC notification.
- Varying notification/escalation per category.

8.5. Change, Maintenance, and Release Management

8.5.1. Change Management Requirements

The Contractor shall ensure that all changes – planned or unplanned – are managed through a structured, documented, and auditable process that maintains service stability, security, and interoperability. The process shall conform to the principles of the **Project Management Institute (PMI)** and the **ITIL v4 Service Management Framework**.

Objectives

The objectives of the Contractor's Change Management process shall be to:

- Maintain a stable and secure NG911 operational environment.
- Minimize the impact of changes on system availability, reliability, and public safety operations.
- Provide transparency and accountability for all system modifications.
- Ensure that all stakeholders are informed, consulted, and prepared for any change that affects service delivery.
- Incorporate continuous improvement through post-implementation review and process enhancement.

The Change Management process shall apply to all infrastructure, applications, systems, and interfaces under Contractor operational control, including but not limited to:

- **ESInet Infrastructure**: routers, firewalls, switches, circuits, transport paths, and interconnections.
- **NGCS Components**: ESRP, ECRF/LVF, PRF, BCF, LIS, logging, and policy routing elements.
- **Call Handling Systems**: software, hardware, operating systems, and integrations with CAD, logging, and recording systems.
- **Security Systems**: encryption, certificates, firewalls, intrusion detection/prevention, and access controls.
- **Support and Management Tools**: monitoring platforms, ticketing systems, and network management applications.

Change Classification

The Contractor shall classify all changes into the following categories:

- **Standard Change**: Pre-approved, low-risk, repeatable changes executed according to pre-established procedures (e.g., routine software patching).
- **Normal Change**: Planned changes that require full evaluation, testing, review, approval, and scheduling.
- **Emergency Change**: Unplanned changes necessary to restore service, mitigate critical vulnerabilities, or prevent imminent service degradation.

Each classification shall have documented criteria, approval authorities, and implementation procedures.

Process Requirements

The Contractor shall implement a formal Change Management process that includes the following elements:

- **Change Management Plan**: A documented process outlining governance, roles, responsibilities, and workflows aligned with PMI and ITIL best practices.
- **Change Advisory Board (CAB)**: A standing review body, including State representation, responsible for evaluating and approving all Normal and Major Changes.
- **Change Request System**: A centralized, auditable tool for logging, tracking, and managing all changes from request through closure.
- **Risk and Impact Assessment**: An analysis of each proposed change to evaluate its impact on system performance, service continuity, interoperability, and cybersecurity.
- **Rollback and Contingency Plans**: Documented procedures for reverting or recovering from unsuccessful change implementations.

- **Change Scheduling and Coordination**: Change windows coordinated with the State and PSAPs to minimize service disruptions.
- **Notification Requirements**: Written notice to affected stakeholders no less than ten (10) business days prior to implementation of any planned change, unless otherwise authorized.
- **Post-Implementation Review (PIR)**: A formal evaluation of significant or failed changes to identify root causes, corrective actions, and process improvements.

Emergency and Security Changes

- The Contractor shall maintain procedures for the execution of emergency changes required to restore service or address urgent security vulnerabilities.
- All emergency changes shall be documented and submitted for retrospective review by the CAB within five (5) business days.
- Security-related changes, including software updates, certificate renewals, or configuration modifications, shall comply with PMI and ITIL Change Enablement best practices.
- Security changes shall be tested in a controlled environment prior to production deployment whenever feasible.
- The Contractor shall notify the State of any emergency or security change within twenty-four (24) hours of implementation.

Integration with Other Service Management Processes

The Contractor shall integrate Change Management with the following processes:

- **Configuration Management**: Each change shall be linked to affected Configuration Items (CIs) within the Configuration Management Database (CMDB).
- **Incident Management**: Changes shall be correlated with incident and problem records to support root cause analysis and continuous improvement.
- **Release and Deployment Management**: The Contractor shall coordinate releases to ensure version control and documentation integrity across environments.

8.5.1.1. Security Considerations in Change Management

In conjunction with the change management processes defined in §E-9.5.2 (Scheduled Maintenance Process) and §E-9.5.3 (Software Update and Improvements) of this document, the contractor must evaluate the **security impact** and **operational risk** for all changes to NGCS elements and the ESInet – including equipment, software, and configurations. Every change requires **policy-compliant review and approval, a documented security review, and complete records**. If timing precludes standard pre-approval (Unplanned/Emergency [time-critical issues with expedited workflows] issues), all required reviews and documentation must be completed immediately after implementation. The contractor should utilize segregation of duties, maintain configuration baselines, and coordinate maintenance windows to protect call delivery, routing, location accuracy, latency, and availability.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Evidence that all changes are reviewed and approved per policy with a documented security review (threat/impact, affected NGCS/ESInet elements and services, potential customer impact, required controls and monitoring).
- An Unplanned/Emergency change process that documents expedited approvals and requires retroactive completion of all "SHALL" requirements and documentation identified in NENA-STA-040.2 §4.4 (Change Management) within a defined timeframe.

8.5.2. Scheduled Maintenance Process

A scheduled maintenance process document will be developed and maintained. The process must include a methodology for coordinating and scheduling preventative maintenance activities and how those events are executed as may be necessary during the operation of the NG911 system.

During scheduled maintenance activities the ESInet and NG911 system must maintain 99.999% availability. There must not be a substantial degradation or disruption caused by the maintenance activity. However, individual components may be taken down for maintenance if an alternate route or redundant system is used to maintain the 99.999% threshold.

If a partial or total outage occurs within hours of a maintenance activity, Contractor shall issue a report within 30 days to the State detailing:

- What occurred during the outage, including system elements that were impacted
- Whether the outage was caused by, or influenced by, the maintenance activity
- What corrective actions, specifically corrective actions to the change control process, will be implemented to avoid recurrence, not just to the specific problem but to similar problems

Following any scheduled maintenance, a maintenance report must be prepared and sent to the State within 24 hours, detailing:

- What are the results of the scheduled maintenance
- What was done during the scheduled maintenance
- How will such scheduled maintenance impact the services in operation

Following any emergency maintenance, an emergency maintenance report must be prepared and sent to the State within 24 hours, detailing:

- What caused the emergency maintenance
- What was done during the emergency maintenance
- How will such emergency maintenance be avoided in the future

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Developed/maintained process document for coordinating/scheduling preventative maintenance.
- No degradation/disruption during activities.
- Allowance for individual component downtime with alternates/redundancy.

8.5.3. Software Development Process

The Contractor and all Subcontractors shall use a documented, modern software development lifecycle (SDLC) that produces high-quality code with minimal delay. At a minimum, the SDLC shall include secure coding standards, peer/code reviews, automated testing, version control, and controlled release management (CI/CD or equivalent).

For all software components directly in the NG911 call path, the Contractor and all Subcontractors shall have a process to evaluate, release, and deploy critical security patches within 72 hours of the patch's public availability. This process shall be rehearsed on a regular cadence, and rehearsal results shall be shared with the State.

When a trouble ticket or outage results in a software bug, a discrepancy report, or a required system change to prevent recurrence, the Contractor shall maintain an online, State-accessible log showing each item, severity, affected components, current status, workaround (if any), and the target fix version and release date. This log shall also include items required to bring the system into conformance with standards such as NENA-STA-010.3(including the Discrepancy Reporting function).

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Modern processes for high-quality code with minimal delay.
- 72-hour release/install for critical security patches with rehearsal/results shared.
- Log of bugs/changes/estimated fixes available online.
- Updates for standards conformance.

8.5.4. Software Updates and Improvements

Updates, bug fixes, and patches must be classified by the contractor as normal or emergency. When any normal hardware or software changes are made to a site, there will be a minimum of 30 days before any hardware or

software changes can be made to any other site. Where more than one instance of a function or service is provided on a site, only one instance can be changed at a time. Where there are both multiple sites and redundant instances per site, one instance may be changed at the first site, at least 30 days must elapse, one instance on another site can be made, at least two weeks must elapse, another instance can be updated, after which at least one week must elapse before the next change.

Emergency bug fixes/patches are not required to meet these minimum times. However, if the contractor determines that an emergency bug fix/patch is necessary, it will transmit a report to the State within 48 hours of such a determination, detailing the problem, the necessary fix, and a valid reason the fix could not be completed in regular software update or bug fix processes.

A prescheduled maintenance window will be negotiated between the contractor and the State. All normal maintenance will take place within that window. Extra-ordinary maintenance processes that require additional time may be scheduled with a minimum of 30 days' notice.

Emergency maintenance can be scheduled with no prior notice, but the State must be notified immediately that such an emergency maintenance is needed, what the estimated duration is and why the emergency maintenance is necessary.

The Respondent must provide a detailed methodology for managing all system updates, including software patches, security updates, configuration changes, and data updates (e.g., GIS data). The process must be structured to minimize service disruption, ensure system integrity, and maintain security. The update process must include procedures for testing, scheduling, deployment, and verification of all changes in the production environment.

A formal process for releasing software updates, bug fixes and improvements, and any changes to the process will be communicated to the State within 30 days of the change being put into practice.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Formal process for updates/fixes/improvements with 30-day notice of changes.
- Classification as normal/emergency.
- Minimum 30-day spacing for normal changes across sites/instances.
- No minimum times for emergency but 48-hour report to State.
- Negotiated maintenance window.
- Extra-ordinary with 30-day notice.
- Immediate notification for emergency with duration/reason.

8.6. Spares and Inventory

8.6.1. Spares

Respondents must describe their spares program, including stocking levels, storage locations, and the time required for an on-site field technician to obtain a spare. If the State has any role in spare stocking or access, explain that role.

A sufficient supply of spare parts shall be maintained at locations that enable immediate restoration of service. This requirement is tied to the Mean Time to Repair (MTTR) specified in §E-9 of this document. Where there are multiple connections, the Contractor shall provide multiple spare units staged in multiple locations.

Within the proposal response, explain how sparing strategies maintain both Mean Time Between Failures (MTBF) and MTTR at levels necessary to achieve 99.999% availability.

If malfunctions or failures recur, the State may require the Contractor to increase spare inventory to ensure adequate parts are available to address the repeated issue.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Describe the spares program, including stocking levels, locations, and technician access time

- Explain any State role in spare stocking or access
- Show how sparing maintains required MTBF/MTTR to achieve 99.999% availability

Operational Obligations (Post-Award):

- Maintain spare inventory at levels consistent with MTTR needs.
- Refresh replacement stock within twenty-four (24) hours after use
- Retain sole responsibility for restocking spare parts
- Track and report monthly on equipment failures requiring use of spare inventory
- Adjust inventory as needed and provide documentation to the State upon request
- Identify where spares are located and maintained
- Use spare inventory to support the entire proposed system, adjusting as needed
- Replenish remote parts depots when their stock is depleted
- Increase spare inventory if repeated malfunctions occur.

8.6.2. Spare Inventory at Data Centers

In addition to the spare inventory maintained at Contractor locations, the Contractor must maintain critical spare inventory on-site at each data center location. The Contractor must:

- Identify and provide documentation of critical spare inventory maintained on-site at each data center
- Add equipment to this list based on frequency and type of repair to ensure critical spare inventory is maintained on-site at all times
- Replenish spare parts inventory if required by the State in case of repeated malfunction or failure

This on-site inventory ensures immediate access to critical components needed to maintain the required system availability.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- On-site critical spare inventory at each data center.
- Identification/documentation of inventory.
- Additions based on repair frequency/type.
- Replenishment for repeated malfunctions/failures.

Remainder of page intentionally blank

9. Value Add and Optional Services

Respondents will describe any optional services that may enhance their product or the delivery of NG911 to the State. Particularly, this may mean the ability to deliver a hosted call handling system after the ESInet has been deployed and NG911 routing is being provided.

9.1. Call Handling Equipment (CHE) Services

The PSC would like to have insight into the options a vendor may provide for CHE. PSAPs in the State may want to move to a hosted solution or an approved solution at some point during the contract period. In order to determine the viability proposers may offer a CHE solution as an option, but it is not a firm requirement at this time.

Hosted CHE is preferred; to allow PSAPs an option of moving from an on-prem call handling system into the hosted CHE platform over time.

The Respondent may provide a Call Handling Equipment (CHE) solution that serves as the primary user interface for PSAP call takers and dispatchers. The CHE must be capable of receiving and managing emergency calls from the ESInet, including support for various media types such as voice, real-time text (RTT), and video. The solution must provide an intuitive graphical user interface (GUI) that displays all pertinent call information, including caller location on a map, and integrates seamlessly with other PSAP systems like Computer Aided Dispatch (CAD) and logging recorders.

Also, the signaling and media interface at the demarcation between the ESInet infrastructure and the PSAP will comply with standards-based NG911 requirements as stated in the NG911 services section and elsewhere within the technical and operational requirements. Solutions that utilize proprietary signaling and/or media across the Access Network to End Site demarcation point, or that otherwise do not comply with the technical or operational requirements specified for this demarcation point, will not be acceptable.

9.2. ESInet and NGCS backup system

The PSC would also like to understand the options a vendor may provide to increase the diversity and redundancy of the system. This may be a tertiary alternative that could be utilized in the event of the primary system or transport failure.

Remainder of page intentionally blank

10. Use Case Examples for Use with Response

10.1. Instructions

The following diagrams depict the NG911 system from a functional view. These Use Case scenarios provide Respondents the opportunity to demonstrate the traffic flow and performance perspectives of their proposed system. The Use Cases are designed to present a basis for validation of responses to the requirements of the RFP and will be used as a basis for evaluation of the delivery of traffic from caller to PSAP.

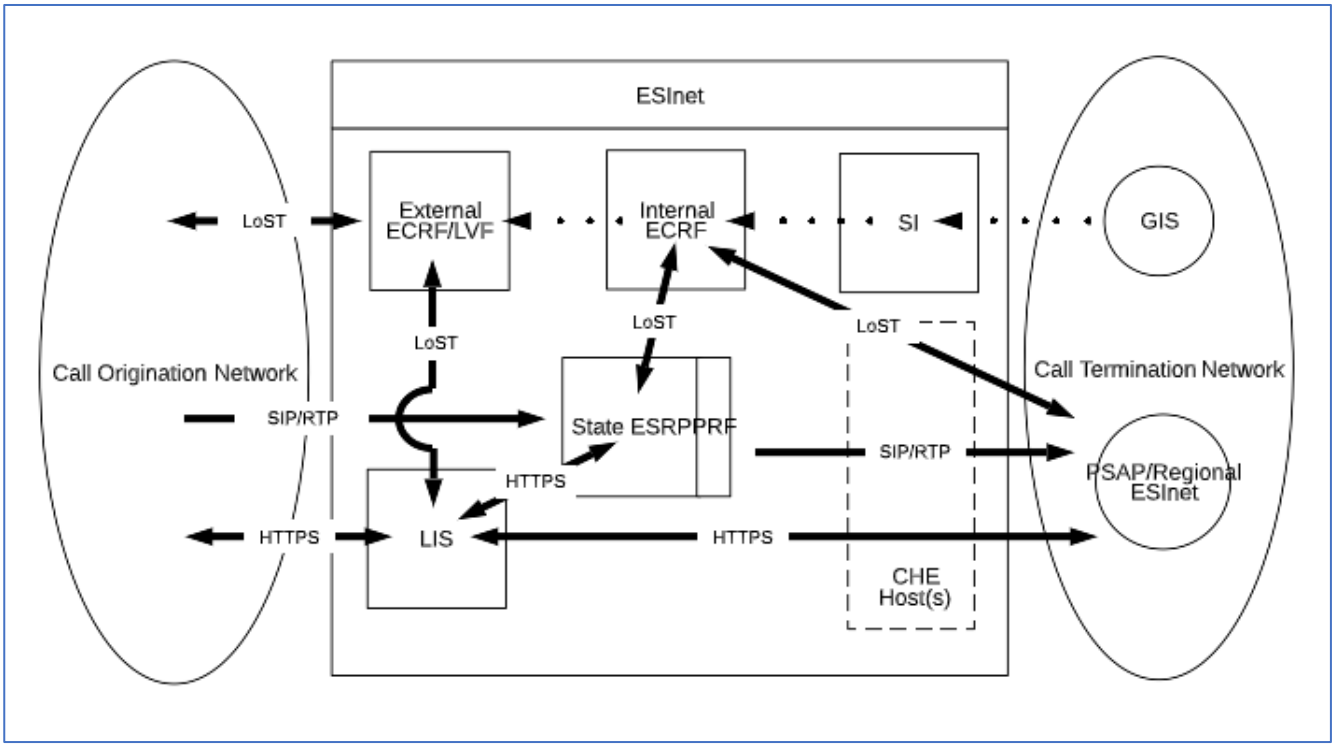


Figure 3: High-level NENA i3v3 Architecture

Remainder of page intentionally blank

High-Level Use Case and Overall Expectation

The first expectation is for the Respondent to offer a narrative of how their proposed solution will meet the functionality depicted in the above diagram.

Respondents must:

- Describe how traffic flows from the call origination network, through the core to the PSAP in step-by-step fashion.
    - At each functional element, a description shall be provided to discuss how the traffic flow is being modified or adjusted due to additional data between functional elements.
    - At each functional element, a description shall be provided to identify how the system is managed and how alerts of disruptions or incidents will automatically notify the NOC.
    - At each functional element, a description of how the interface between the functional elements will be utilized.
    - Demonstrate how the system will handle the use case presented and discuss the operation, including which partner(s) (Prime or Subcontractor) would be responsible for ingress, core, and egress.
    - Identify the bandwidth available and options to manage and monitor bandwidth between functional elements and for the entire platform.
- Describe the performance expectations of the system and explain how performance is guaranteed for legacy 911 across the entire system to egress to a legacy PSAP.
    - Identify how systems operate in a “normal” state.
    - Identify how systems operate in an “abnormal” condition.
    - Demonstrate how the platform will operate in a “fail” condition.
- Describe how security is implemented across the system while maintaining the performance guarantees expected to egress to a legacy PSAP.
    - Identify how DDoS and TDoS events are mitigated.
    - Identify how security events are mitigated at each component throughout the system, including incidents that derive from the OSP, the PSAP and other ESInets.
- Describe how 911 data is delivered to the logging and reporting system to be accessed by a PSAP.
    - Identify how databases operate.
    - Explain how recording systems are implemented to accommodate local recording and to accommodate hosted recording.
    - Explain how logging is collected and accessed for legacy CDR and i3 logging.
- Describe how calls may be transferred between NG PSAPs.
    - Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on the same NG911 system.
    - Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on a different NG911 system.
    - Describe how transfers are logged and how the data is logged.
    - Discuss the data that is transferred to the receiving PSAP.
    - Explain how logging is collected and accessed for legacy CDR and i3 logging
- Describe any areas where the “span of control” on enforcement of diversity, redundancy, policies, procedures or any other automated or manual function that would limit the overall success of a call reaching a call taker is within the system.
    - Explain the limitations with the proposed system in a clear manner so that the evaluation team, and the State have a clear understanding of what is being proposed.
    - Gaps and limitations do not disqualify or eliminate a proposal; on the contrary an open and honest response will allow these types of issues to be documented and will lead to a collaborative plan to remediate.

Remainder of page intentionally blank

10.2. Additional Examples

The following diagrams serve as an example of how a Respondent shall answer the use case questions. Diagrams may be necessary with step-by-step demonstration callouts to document the overall traffic flow for the system. Respondents are encouraged to use their own diagram(s) to illustrate the traffic flow from end to end.

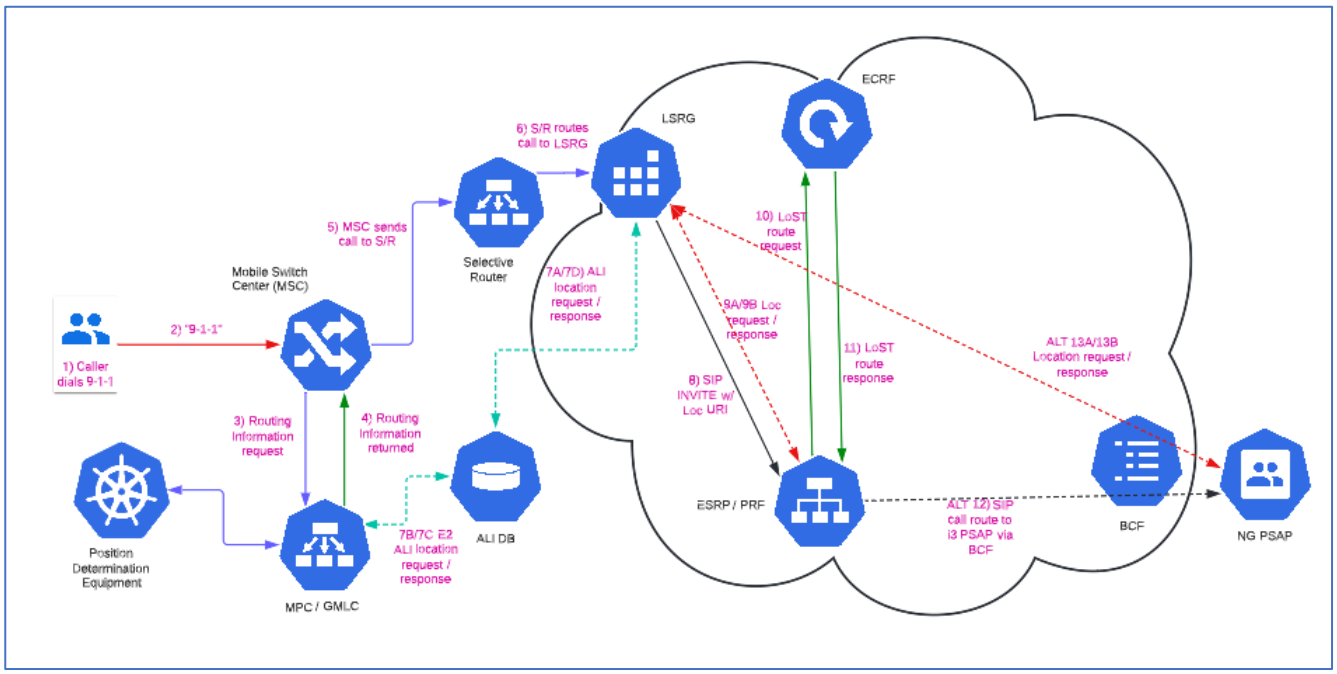
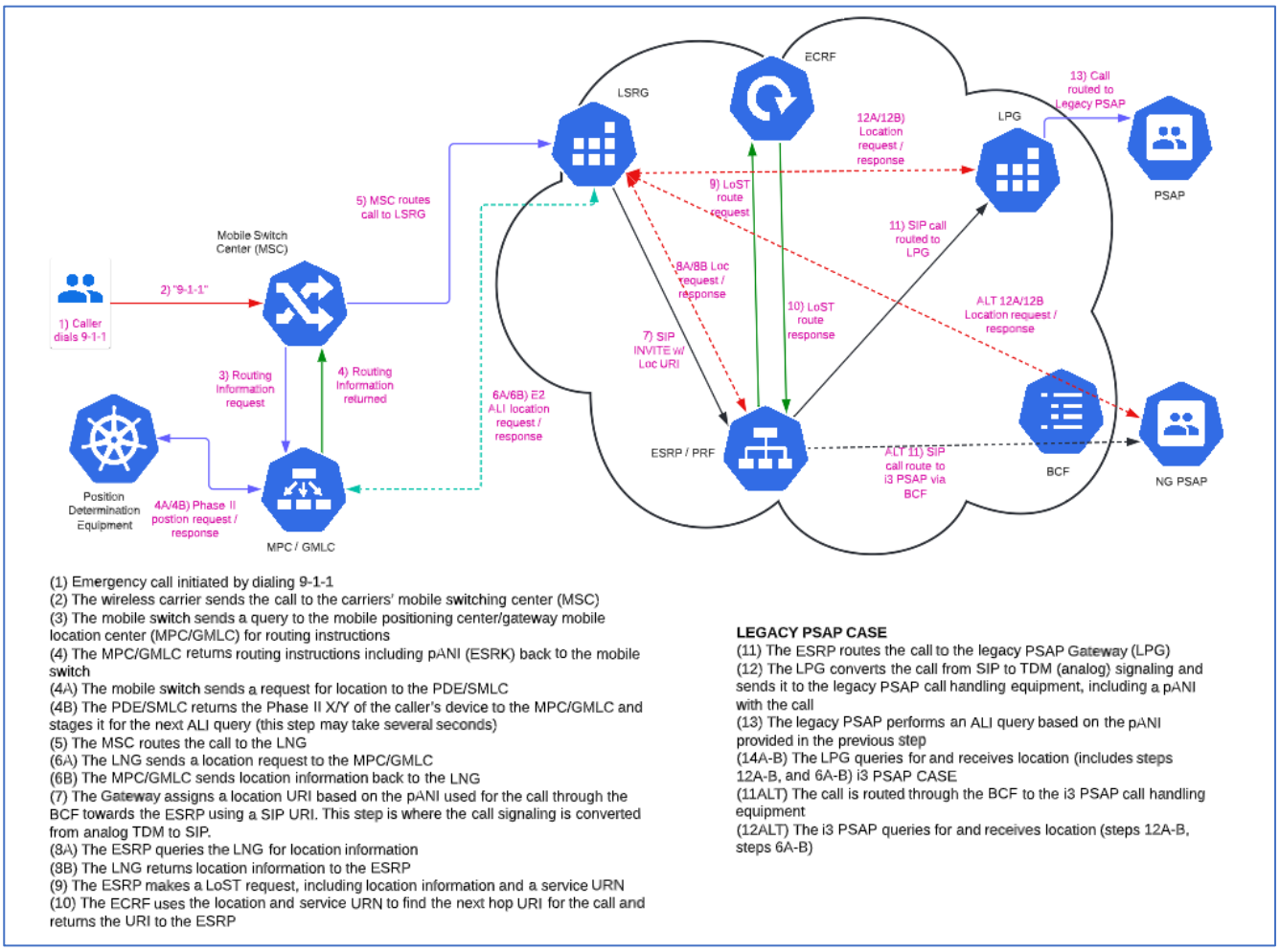


Figure 4: NENA Call Flow Scenario 1

Remainder of page intentionally blank



(1) Emergency call initiated by dialing 9-1-1
(2) The wireless carrier sends the call to the carriers' mobile switching center (MSC)
(3) The mobile switch sends a query to the mobile positioning center/gateway mobile location center (MPC/GMLC) for routing instructions
(4) The MPC/GMLC returns routing instructions including pANI (ESRK) back to the mobile switch
(4A) The mobile switch sends a request for location to the PDE/SMLC
(4B) The PDE/SMLC returns the Phase II X/Y of the caller's device to the MPC/GMLC and stages it for the next ALI query (this step may take several seconds)
(5) The MSC routes the call to the LNG
(6A) The LNG sends a location request to the MPC/GMLC
(6B) The MPC/GMLC sends location information back to the LNG
(7) The Gateway assigns a location URI based on the pANI used for the call through the BCF towards the ESRP using a SIP URI. This step is where the call signaling is converted from analog TDM to SIP.
(8A) The ESRP queries the LNG for location information
(8B) The LNG returns location information to the ESRP
(9) The ESRP makes a LoST request, including location information and a service URN
(10) The ECRF uses the location and service URN to find the next hop URI for the call and returns the URI to the ESRP

LEGACY PSAP CASE
(11) The ESRP routes the call to the legacy PSAP Gateway (LPG)
(12) The LPG converts the call from SIP to TDM (analog) signaling and sends it to the legacy PSAP call handling equipment, including a pANI with the call
(13) The legacy PSAP performs an ALI query based on the pANI provided in the previous step
(14A-B) The LPG queries for and receives location (includes steps 12A-B, and 6A-B) i3 PSAP CASE
(11ALT) The call is routed through the BCF to the i3 PSAP call handling equipment
(12ALT) The i3 PSAP queries for and receives location (steps 12A-B, steps 6A-B)

Figure 5: NENA Call Flow Scenario 2

Remainder of page intentionally blank

Procurement Procedure

A. GENERAL INFORMATION

This solicitation is designed to solicit responses from qualified bidders who will be responsible for providing the service described in this RFP at a competitive and reasonable cost. This **Procurement Procedure** describes how the solicitation will be conducted through bidding and contract award.

The Commission reserves the right to reject a bidder's solicitation response, withdraw an Intent to Award, or terminate a contract if the Commission determines there has been a violation of this Procurement Procedure.

B. PROCURING OFFICE AND COMMUNICATION WITH STATE STAFF AND EVALUATORS

Procurement responsibilities related to this solicitation reside with the Commission. Please note, again, that the Department of Administrative Services is not a contact for anything related to this solicitation. The point of contact (POC) for the procurement is as follows:

RFP Number:	RFP 202691101
Name:	**David Sankey – State 911 Director**
Agency:	Nebraska Public Service Commission
Address:	1200 N Street, Suite 300
	Lincoln, NE 68508
Telephone:	402-471-3101
E-Mail:	**dave.sankey@nebraska.gov**

From the date the solicitation is issued until the Intent to Award is issued, communication from the bidder about or concerning this RFP is limited to the POC listed above. Furthermore, Bidders shall not have any communication with or attempt to communicate or influence any evaluator involved in this solicitation.

After the Intent to Award is issued, the bidder may communicate with individuals the Commission has designated as responsible for negotiating the contract on behalf of the Commission, or pursuant to any protest process. No Commissioner, member of the State Government, employee of the State, or member of the Evaluation Committee is empowered to make binding statements regarding this solicitation. The POC will issue any answers, clarifications, or amendments regarding this solicitation in writing.

The following exceptions to these restrictions are permitted:

1. Contact required by the schedule of events or an event scheduled later by the POC; and

2. Contact required for negotiation and execution of the final contract.

C. SCHEDULE OF EVENTS

The Commission expects to adhere to the procurement schedule shown below, but all dates are approximate and subject to change.

(section continues next page)

Remainder of page intentionally blank

Schedule of Events		
ACTIVITY		**DATE/TIME**
1.	Release solicitation	**February 10, 2026**
2.	Last day to submit "Intent to Attend Solicitation Conference" ShareFile link for uploading Notification of Intent to Attend Solicitation Conference: Intent to Attend Solicitation Conference ShareFile	**February 23, 2026**
3.	Last day to submit written questions. ShareFile link for uploading questions: Pre-Conference Written Question Submissions	**February 23, 2026**
4.	**Mandatory** Solicitation Conference Location: Nebraska Public Service Commission 1200 N Street The Atrium Suite 300 Lincoln, NE 68508 ** Registration Advisement:* *Solicitation Responses will only be accepted from those Companies/Firms which properly register their attendance at this meeting by completing all of the required information on the Commission Registration Sheet.*	**March 2, 2026**
5.	Last day to submit written questions after Solicitation Conference ShareFile link for uploading questions: Post-Conference Written Question Submissions	**March 6, 2026**
6.	State responds to written questions through solicitation "Addendum" to be posted to the Internet at: http://das.nebraska.gov/materiel/bidopps.html	**March 13, 2026**

Schedule of Events		
ACTIVITY		**DATE/TIME**
7.	Electronic Solicitation Opening – Online Via Webex IT IS THE BIDDER'S RESPONSIBILTY TO UPLOAD ELECTRONIC FILES BY OPENING DATE AND TIME. EXCEPTIONS WILL NOT BE MADE FOR TECHNOLOGY ISSUES. ShareFile Electronic Solicitation Submission Link: Electronic Solicitation Submissions Join Webex Meeting Meeting link: https://sonvideo.webex.com/meet/State911DepartmentWebex Meeting number: 2495 447 8488 Join from a video conferencing system or application Dial: State911DepartmentWebex@sonvideo.webex.com You can also dial 173.243.2.68 and enter your meeting number. Join by phone +1-408-418-9388 United States Toll Access Code: 2495 447 8488 Global call-in numbers https://sonvideo.webex.com/sonvideo/globalcallin.php?MTID=ma190400aac604f0070dcd9dd5d31e1e9	**March 25, 2026** **2:00 PM** **Central Time**
8.	Review for conformance to solicitation requirements	**March 25, 2026**
9.	Evaluation period	**March 25, 2026, to May 8, 2026**
10.	"Vendor Demonstrations" (if required)	**April 29, 2026**
11.	Post "Notification of Intent to Award" to Internet at: https://das.nebraska.gov/materiel/bidopps.html	**May 15, 2026**
12.	Contract finalization period	**June 12, 2026**
13.	Contract award	**June 17, 2026**
14.	Vendor start date	**June 22, 2026**

D. WRITTEN QUESTIONS AND ANSWERS

Questions regarding the meaning or interpretation of any solicitation provision must be submitted in writing to the Commission and clearly marked "Solicitation Number 202691101; Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) Questions." The POC is not obligated to respond to all questions.

Bidders should submit questions for any items identified when preparing a response to the solicitation. Any solicitation response containing assumptions may be deemed non-responsive and may be rejected by the Commission. Solicitation responses will be evaluated without consideration of any known or unknown assumptions of a bidder. The contract will not incorporate any known or unknown assumptions of a bidder.

Questions should be uploaded using the ShareFile link provided in the solicitation Schedule of Events.

It is recommended that bidders submit questions using the following format:

RFP Section Reference	RFP Page Number	Question

Written answers will be posted at https://das.nebraska.gov/materiel/bidopps.html per the Schedule of Events.

E. SOLICITATION CONFERENCE

A solicitation conference will be held per the Schedule of Events. Attendance at the solicitation conference is mandatory in order to submit a solicitation response, Vendors will have an opportunity to ask questions at the conference to assist in the clarification and understanding of the solicitation requirements. Questions that have a material impact on the solicitation or solicitation process, and relevant to all vendors will be answered in writing and posted at https://das.nebraska.gov/materiel/bidopps.html. An answer must be posted to be binding on the Commission. The Commission will attempt to provide verbal answers to questions that do not impact the solicitation or process, and are only of interest to an individual vendor during the conference. If a vendor feels it necessary to have a binding answer to a question that was answered verbally, the question should be submitted in writing per the SCHEDULE OF EVENTS.

F. NOTICE OF INTENT TO ATTEND MANDATORY SOLICITATION CONFERENCE

Vendors should notify the Commission of their intent to attend by emailing the RFP POC as provided above. Notification is itself not mandatory, even if attendance at the Solicitation Conference is.

G. SECRETARY OF STATE/TAX COMMISSIONER REGISTRATION REQUIREMENTS (Nonnegotiable)

All bidders must be authorized to transact business in the State of Nebraska and comply with all Nebraska Secretary of State Registration requirements. The bidder who is the recipient of an Intent to Award may be required to certify that it has complied and produce a true and exact copy of its current (within ninety (90) calendar days of the Intent to Award) Certificate or Letter of Good Standing, or in the case of a sole proprietorship, provide written documentation of sole proprietorship and complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at:

https://das.nebraska.gov/materiel/docs/pdf/Individual%20or%20Sole%20Proprietor%20United%20States%20Attestation%20Form%20English%20and%20Spanish.pdf This should be accomplished prior to execution of the contract.

H. ETHICS IN PUBLIC CONTRACTING

The Commission reserves the right to reject solicitation responses or withdraw an Intent to Award if an ethical violation has been committed, which includes, but is not limited to:

1. Offering or giving, directly or indirectly, a bribe, fee, commission, compensation, gift, gratuity, or anything of value to any person or entity in an attempt to influence the bidding process;
2. Utilizing the services of lobbyists, attorneys, political activists, or consultants to influence or subvert the bidding process;
3. Being considered for, presently being, or becoming debarred, suspended, ineligible, or excluded from contracting with any state or federal entity:
4. Submitting a solicitation response on behalf of another Party or entity; and
5. Colluding with any person or entity to influence the bidding process, submit sham solicitation responses, preclude bidding, fix pricing or costs, create an unfair advantage, subvert the solicitation response, or prejudice the Commission.

Bidder shall have an affirmative duty to report any violations of this clause by the bidder throughout the bidding process for the awarded bidder and their subcontractors.

I. DEVIATIONS FROM THE SOLICITATION

Any deviations from the standards in the Scope of Work must be clearly defined by the bidder in its solicitation response and, if accepted by the Commission, will become part of the contract in the harmonization process. Any specifically defined deviations must not be in conflict with the basic nature of the solicitation, requirements, or applicable state or federal laws or statutes. The Commission discourages deviations and reserves the right to reject proposed deviations.

J. SUBMISSION OF SOLICITATION RESPONSES

The Commission is only accepting electronic responses submitted in accordance with this solicitation. The State will not accept solicitation responses by mail, email, voice, or telephone, unless otherwise explicitly stated in writing by the Commission.

It is the bidder's responsibility to ensure the solicitation response is received electronically by the date and time indicated in the Schedule of Events. Solicitation Responses must be submitted via ShareFile by the date and time of the opening per the Schedule of Events. No late solicitation responses will be accepted.

It is the responsibility of the bidder to check the website for all information relevant to this solicitation to include addenda and/or amendments issued prior to the opening date. The website can be found here: https://das.nebraska.gov/materiel/bidopps.html.

The ShareFile link for uploading Solicitation Response(s) is provided in the SCHEDULE OF EVENTS

*****UNLESS OTHERWISE NOTED, DO NOT SUBMIT DOCUMENTS**

THAT CAN ONLY BE ACCESSED WITH A PASSWORD***

1. **Bidders must submit responses via ShareFile using the solicitation submission link.**
   Note: Not all browsers are compatible with ShareFile. Currently Chrome, Internet Explorer and Firefox are compatible. After the bidder clicks the solicitation response submission link, the bidder will be prompted to enter contact information including an e-mail address. By entering an e-mail address, the bidder should receive a confirmation email confirming the successful upload directly from ShareFile.

   ShareFile link for uploading solicitation response(s) provided in the SCHEDULE OF EVENTS

   a. The Solicitation response and Proprietary information should be uploaded as separate and distinct files.

      i. If duplicated responses are submitted, the Commission will retain only the most recently submitted response.
      ii. If it is the bidder's intent to submit multiple responses, the bidder must clearly identify the separate submissions.

iii. It is the bidder's responsibility to allow time for electronic uploading. All file uploads must be completed by the Opening date and time per the Schedule of Events. No late responses will be accepted.

b. ELECTRONIC SOLICITATION RESPONSE FILE NAMES

The bidder should clearly identify the uploaded solicitation response files. To assist in identification the bidder should use the following naming convention:

i. 202691101, Company Name

ii. If multiple files are submitted for one solicitation response, add number of files to file names:

a) 202691101 Company Name File 1 of 2.
b) 202691101 Company Name File 2 of 2.

iii. If multiple responses are submitted for the same solicitation, add the response number to the file names:

a) 202691101 Company Name Response 1 File 1 of 2.
b) 202691101 Company Name Response 2 File 1 of 2.

K. SOLICITATION PREPARATION COSTS

The Commission shall not incur any liability for any costs incurred by bidder's in replying to this solicitation, including any activity related to bidding on this solicitation.

L. FAILURE TO COMPLY WITH SOLICITATION

Violation of the terms and conditions contained in this solicitation, at any time before or after the award, shall be grounds for action by the Commission, which may include, but is not limited to, the following:

1. Rejection of a bidder's solicitation response,
2. Withdrawal of the Intent to Award,
3. Withdrawal of the Award,
4. Negative documentation regarding Vendor Performance,
5. Legal action; and
6. Suspension or Debarment of the bidder from further bidding with the Commission or the State for a period of time relative to the seriousness of the violation. Such period to be within the sole discretion of the State.

M. SOLICITATION RESPONSE CORRECTIONS

A bidder may correct a mistake in an electronically submitted solicitation response prior to the time of opening by uploading a revised and completed solicitation response.

1. If a corrected electronic solicitation response is submitted, the file name(s) date/time stamped with latest date/time stamp will be accepted. The corrected solicitation response file name(s) should be identified as:
   a. Corrected XXXX Z1 Company Name Response #1 File 1 of 2,
   b. Corrected XXXX Z1 Company Name Response #2 File 2 of 2, etc.

Changing a solicitation response after opening may be permitted if the change is made to correct a minor error that does not affect price, quantity, quality, delivery, or contractual conditions.

N. LATE SOLICITATION RESPONSES

Solicitation Responses received after the time and date of the opening will be considered late responses. Late responses will be considered non-responsive. The Commission is not responsible for responses that are late or lost regardless of cause or fault.

O. BID OPENING

The opening will consist of opening solicitation responses and announcing the names of bidders. Responses **WILL NOT** be available for viewing by those present at the opening. Responses will be posted to the DAS website once an Intent to Award has been posted to the website. Once responses are opened, they become the property of the State of Nebraska and will not be returned.

P. SOLICITATION REQUIREMENTS

The solicitation responses will first be examined by the POC to determine if all requirements listed below have been addressed and whether further evaluation is warranted (i.e., whether the solicitation response is responsive).

Q. EVALUATION OF RESPONSES

Solicitation Responses deemed responsive are evaluated by members of an Evaluation Committee(s). The Evaluation Committee(s) will consist of individuals selected at the discretion of the Commission. Names of the members of the Evaluation Committee(s) will not be published prior to the Intent to Award.

Any contact, attempted contact, or attempt to influence an evaluator that is involved with this solicitation may result in the rejection of this response and further administrative actions.

The Commission will conduct a fair, impartial, and comprehensive evaluation of all responses in accordance with the criteria set forth in the Proposal Instructions, below. The Commission may elect to use a third party to conduct credit checks as part of the corporate overview evaluation.

Each evaluation category will have a maximum point potential, as follows:

Evaluation Criteria	
Part 1 – Corporate Overview	25
Part 2 – Response to Scope of Work, Work Plan and Project Planning, Deliverables, and Technical Requirements	60
Part 3 – Cost	10
Total Points without Oral Interviews	95
Oral Interviews, (if required)	5
Total Points with Oral Interviews	100

R. BEST AND FINAL OFFER

Each bidder should provide its best offer with their original solicitation response and should not expect the Commission to request a best and final offer (BAFO).

The Commission reserves the right to conduct more than one BAFO. If requested by the Commission, the BAFO must be submitted on the BAFO Cost Sheet and in accordance with the Commission's instructions. Failure to submit a requested BAFO or failure to submit a BAFO in accordance with the Commission's instructions may result in rejection of the bidder's entire solicitation response. BAFOs may be scored and ranked by the Evaluation Committee.

S. REFERENCE AND CREDIT CHECKS

The Commission reserves the right to conduct and consider reference and credit checks. The Commission reserves the right to use third parties to conduct reference and credit checks. By submitting a solicitation response, the bidder grants to the

Commission the right to contact or arrange a visit in person with any or all of the bidder's clients. Reference and credit checks may be grounds to reject a solicitation response, withdraw an intent to award, or rescind the award of a contract.

T. AWARD

The Commission reserves the right to evaluate solicitation responses and award contracts in a manner utilizing criteria selected at the Commission's discretion and in the Commission's best interest. After evaluation of the solicitation responses, or at any point in the solicitation process, the Commission may take one or more of the following actions:

1. Amend the solicitation;
2. Extend the date and time of a solicitation;
3. Waive deviations or errors in the Commission's solicitation process and in bidder responses that are not material, do not compromise the solicitation process or a bidder's response, and do not improve a vendor's competitive position;
4. Accept or reject a portion of or all of a solicitation response;
5. Accept or reject all responses;
6. Withdraw the solicitation;
7. Elect to re-release the solicitation;
8. Award single lines or multiple lines to one or more Vendors; or,
9. Award one or more all-inclusive contracts.

The solicitation does not commit the Commission to award a contract. Once intent to award decision has been determined, it will be posted to the Internet at: https://das.nebraska.gov/materiel/bidopps.html

Only the Commission, after a vote by a majority of the Commissioners at a public meeting, can award a contract from this RFP.

U. REJECTION OF SOLICITATION RESPONSES

The Commission reserves the right to reject any or all responses, wholly or in part, in the best interest of the Commission.

V. PRICES & COST CLARIFICATION

The Commission reserves the right to review all aspects of cost for reasonableness and realism. To determine, this Commission will use the definitions found in Neb. Rev. Stat. § 73-810 (1) (a) and (b). The Commission may request clarification of any solicitation where the cost component indicates a significant and unsupported deviation from industry standards or in areas where detailed pricing is required. The Commission may reject a bid if the price is not reasonable or realistic.

W. BIDDER DEMONSTRATIONS

The Commission may determine whether oral interviews or presentations or demonstrations are required. Every bidder may not be given an opportunity to interview/present or give demonstrations; the Commission reserves the right, in its discretion, to select only the top scoring bidders to present or give oral interviews.

The presentation process will allow the bidders to demonstrate their solicitation response offering, explaining, or clarifying any unusual or significant elements related to their solicitation responses. Bidders' key personnel, identified in their solicitation response, may be requested to participate in a structured interview to determine their understanding of the requirements of this solicitation response, their authority and reporting relationships within their firm, and their management style and philosophy. Only representatives of the Commission and the presenting bidder will be permitted to attend the oral interviews or presentations or demonstrations. A written copy or summary of the presentation, and demonstrative information (such as briefing charts) may be offered by the bidder, but the Commission reserves the right to refuse or not consider the offered materials. Bidders shall not be allowed to alter or amend their solicitation responses.

Once the oral interviews/presentations and/or demonstrations have been completed, the Commission reserves the right to make an award without any further discussion with the bidders regarding the solicitation responses received.

Any cost incidental to the oral interviews/presentations and/or demonstrations shall be borne entirely by the bidder and will not be compensated by the Commission.

The scores from the oral interviews or presentations or demonstrations will be added to the scores from the Corporative Overview, Response to Project Requirements and Scope of Work, and Cost Proposal.

X. EFFECT OF RFP

In the event that a contract with the awarded bidder(s) is cancelled or in the event that the Commission needs additional Vendors to supply the solicited services, this RFP may be used to procure the solicited services for (choose how long procurement can be used – may not exceed two (2) years from the Intent to Award) up to eighteen (18) months from the date the Intent to Award is posted, provided that 1) the solicited goods or services will be provided by a bidder (or a successive owner) who submitted a response pursuant to this solicitation, 2) the bidder's solicitation response was evaluated, and 3) the bidder will honor the bidder's original solicitation response, including the proposed cost, allowing for any price increases that would have otherwise been allowed if the bidder would have received the initial award.

Y. WAIVER OF COPYRIGHT AND ACKNOWLEDGEMENT OF PUBLIC POSTING

To facilitate public posting of any solicitation responses, the State of Nebraska reserves a royalty-free, nonexclusive, and irrevocable right to copy, reproduce, publish, post to a website, or otherwise use any contract, or solicitation response for any purpose, and to authorize others to use the documents. This reservation (and the waiver below) does not include proprietary information.

Any individual or entity awarded a contract, or who submits a solicitation response, specifically waives any copyright or other protection the contract, or solicitation response, may have; and acknowledges that they have the ability and authority to enter into such waiver. This reservation and waiver are a prerequisite for submitting a solicitation response, and award of a contract. Failure to agree to the reservation and waiver will result in the solicitation response being found non-responsive and rejected.

Any entity awarded a contract or submitting a solicitation response agrees not to sue, file a claim, or make a demand of any kind, and will indemnify and hold harmless the State and its employees, volunteers, agents, and its elected and appointed officials from and against any and all claims, liens, demands, damages, liability, actions, causes of action, losses, judgments, costs, and expenses of every nature, including investigation costs and expenses, settlement costs, and attorney fees and expenses, sustained or asserted against the State, arising out of, resulting from, or attributable to the posting of the contract or solicitation response, awards, and other documents.

Z. CONTRACT FINALIZATION PROCESS AND TERMS NEGOTIATION

As provided in the **Proposal Instructions**, below, the bidder must submit a response to the Commission's proposed terms. After the Intent to Award is issued, the Commission will contact the winning bidder to finalize the contract. Finalization of contract will include any negotiation of terms for which the bidder noted exceptions when it submitted its solicitation response, as well as incorporation of any other changes based on errors or ambiguities identified in the written Q&A.

The final scope of work will harmonize any differences between the Scope of Work in the RFP and the bidder's proposal, although it may not expand upon the scope of the original RFP or provide the winning bidder with any chances to modify their proposal and achieve any kind of competitive advantage over other bidders. The harmonization process will only streamline the glossary, scope of work and deliverables to ensure the Commission has clearly defined contractual obligations and deliverables.

The Commission reserves the right to negotiate rejected or proposed alternative language provided by bidder in its response to the term sheet or provided in this stage of the bidding process. If the Commission and bidder fail to agree on the final Terms and Conditions, the Commission reserves the right to reject the solicitation response. The Commission also reserves the right to reject solicitation responses that attempt to substitute the bidder's commercial contracts or documents for this solicitation.

The contract resulting from this RFP will be made up of the following documents:

1. Contract Award (generated by Commission after award);
2. Glossary;
3. Final, harmonized Scope of Work (including any deliverables);
4. Cost Proposal;
5. Relevant attachments from the RFP or solicitation response, if not otherwise incorporated into Scope of Work; and

6. Negotiated Terms.

The rest of the RFP will not be included unless agreed by the parties to be necessary to ensure clear contractual provisions in the Scope of Work.

Pursuant to Neb. Rev. Stat. § 84-602.04, the final Contract must be posted to a public website. The resulting contract will be posted to a public website managed by DAS, which can be found at http://statecontracts.nebraska.gov and https://www.nebraska.gov/das/materiel/purchasing/contract_search/index.php.

The resulting contract may not be an exclusive contract as the Commission reserves the right to contract for the same or similar services from other sources now or in the future.

AA. PROTESTS

Protests of the specifications contained in the RFP must be filed no later than ten (10) business days after the solicitation has been posted publicly. Protests of the Intent to Award must be filed by a bidder within ten (10) business days after the intent to award decision is posted to the Internet.

Grievance and protest procedure for the Commission, including where to submit protests, is available on the Internet at: psc.nebraska.gov. The guidance document is located on the Administration page.

BB. DEBRIEFINGS

A bidder may request a debriefing with the Commission after the protest period of an Intent to Award has lapsed. The request must be received by the POC no later than sixty (60) calendar days after the Intent to Award has been posted to the website. In response to the debriefing request, Commission may either (1) Refuse; or (2) Respond in writing, with an explanation as to why the bidder did not receive the award; or (3) The Commission may meet with the bidder, either in person or through videoconferencing. In any case, the Commission is not required to disclose any information not otherwise required to be disclosed by law, and by agreeing to a debriefing, the Commission does not waive any rights, privileges, or immunities.

Remainder of page intentionally blank

Proposal Instructions

Proposals must conform to all instructions, conditions, and requirements included in this RFP. Prospective bidders are expected to carefully examine all documents, schedules, and requirements in this solicitation, and respond to each requirement in the format prescribed. Solicitation responses may be found non-responsive if they do not conform to the solicitation. Emphasis should be concentrated on conformance to the solicitation instructions, responsiveness to requirements, completeness, and clarity of content.

Bidders must provide the following:

1. Corporate Overview;
2. Response to Scope of Work;
3. Response to Work Plan and Project Planning;
4. Response to Technical Requirements;
5. Cost Sheet;
6. Response to Terms;
7. Contractual Agreement Form; and
8. Any other specific requested items below.

Bidders should identify each item clearly in their solicitation response; failure to do so, or to present the response in such a fashion that makes evaluation difficult or overly time consuming, may result in disqualification. Failure to respond to a specific requirement may also be the basis for elimination from consideration during the Commission's comparative evaluation.

Where the below requirements stipulate a disclosure to be made, such as in Contract Performance, a failure to fully disclose, if determined by the Commission, may result in elimination from consideration. This is in the discretion of the Commission.

A. SOLICITATION RESPONSE SUBMISSION

1. CORPORATE OVERVIEW

The Corporate Overview section of the solicitation response should consist of the following subdivisions:

a. BIDDER IDENTIFICATION AND INFORMATION

The bidder should provide the full company or corporate name, address of the company's headquarters, entity organization (corporation, partnership, proprietorship), state in which the bidder is incorporated or otherwise organized to do business, year in which the bidder first organized to do business and whether the name and form of organization has changed since first organized.

b. FINANCIAL STATEMENTS

The bidder should provide financial statements applicable to the firm. If publicly held, the bidder should provide a copy of the corporation's most recent audited financial reports and statements, and the name, address, and telephone number of the fiscally responsible representative of the bidder's financial or banking organization.

If the bidder is not a publicly held corporation, either the reports and statements required of a publicly held corporation, or a description of the organization, including size, longevity, client base, areas of specialization and expertise, and any other pertinent information, should be submitted in such a manner that solicitation evaluators may reasonably formulate a determination about the stability and financial strength of the organization. Additionally, a non-publicly held firm should provide a banking reference.

The bidder must disclose any and all judgments, pending or expected litigation, or other real or potential financial reversals, which might materially affect the viability or stability of the organization, or state that no such condition is known to exist.

c. CHANGE OF OWNERSHIP

If any change in ownership or control of the company is anticipated during the twelve (12) months following the solicitation response due date, the bidder should describe the circumstances of such change and

indicate when the change will likely occur. Any change of ownership to an awarded bidder(s) will require notification to the Commission.

d. OFFICE LOCATION

The bidder's office location responsible for performance pursuant to an award of a contract with the State of Nebraska should be identified.

e. RELATIONSHIPS WITH THE STATE

The bidder should describe any dealings with the State over the previous ten (10) years. If the organization, its predecessor, or any Party named in the bidder's solicitation response has contracted with the State, the bidder should identify the contract number(s) and/or any other information available to identify such contract(s). If no such contracts exist, so declare.

f. BIDDER'S EMPLOYEE RELATIONS TO STATE

If any Party named in the bidder's solicitation response is or was an employee of the State of Nebraska within the past six (6) months, identify the individual(s) by name, State agency with whom employed, job title or position held with the State, and separation date. If no such relationship exists or has existed, so declare.

If any employee of any agency of the State is employed by the bidder or is a subcontractor to the bidder, as of the due date for solicitation response submission, identify all such persons by name, position held with the bidder, and position held with the State (including job title and agency). Describe the responsibilities of such persons within the proposing organization. If, after review of this information by the State, it is determined that a conflict of interest exists or may exist, the bidder may be disqualified from further consideration in this solicitation. If no such relationship exists, so declare.

g. CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past ten (10) years, all such instances must be described as required below. Termination for default is defined as a notice to stop performance delivery due to the bidder's non-performance or poor performance, and the issue was either not litigated due to inaction on the part of the bidder or litigated and such litigation determined the bidder to be in default.

It is mandatory that the bidder submit full details of all termination for default experienced during the past ten (10) years, including the other Party's name, address, and telephone number. The response to this section must present the bidder's position on the matter. The State will evaluate the facts and will score the bidder's solicitation response accordingly. If no such termination for default has been experienced by the bidder in the past ten (10) years, so declare.

If at any time during the past five (5) years, the bidder has had a contract terminated for convenience, non-performance, non-allocation of funds, or any other reason, describe fully all circumstances surrounding such termination, including the name and address of the other contracting Party.

h. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

The bidder should provide a summary matrix listing the bidder's previous projects similar to this Solicitation in size, scope, and complexity. The State will use no more than three (3) narrative project descriptions submitted by the bidder during its evaluation of the solicitation response.

The bidder should address the following:

i. Provide narrative descriptions to highlight the similarities between the bidder's experience and this Solicitation. These descriptions should include:

a) The time period of the project,

b) The scheduled and actual completion dates,
c) The bidder's responsibilities,
d) For reference purposes, a customer name (including the name of a contact person, a current telephone number, a facsimile number, and e-mail address); and
e) Each project description should identify whether the work was performed as the prime vendor or as a subcontractor. If a bidder performed as the prime vendor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.

ii. Bidder and Subcontractor(s) experience should be listed separately. Narrative descriptions submitted for Subcontractors should be specifically identified as subcontractor projects.

iii. If the work was performed as a subcontractor, the narrative description should identify the same information as requested for the bidders above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

i. SUMMARY OF BIDDER'S PROPOSED PERSONNEL/MANAGEMENT APPROACH

The bidder should present a detailed description of its proposed approach to the management of the project.

The bidder should identify the specific professionals who will work on the Commission's project if their company is awarded the contract resulting from this solicitation. The names and titles of the team proposed for assignment to the Commission project should be identified in full, with a description of the team leadership, interface, and support functions, and reporting relationships. The primary work assigned to each person should also be identified.

The bidder should provide resumes for all personnel proposed by the bidder to work on the project. The Commission will consider the resumes as a key indicator of the bidder's understanding of the skill mixes required to carry out the requirements of the solicitation in addition to assessing the experience of specific individuals.

Resumes should not be longer than three (3) pages. Resumes should include, at a minimum, academic background and degrees, professional certifications, understanding of the process, and at least three (3) references (name, address, and telephone number) who can attest to the competence and skill level of the individual. Any changes in proposed personnel shall only be implemented after written approval from the Commission.

j. SUBCONTRACTORS

If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide:

i. name, address, and telephone number of the subcontractor(s),
ii. specific tasks for each subcontractor(s),
iii. percentage of performance hours intended for each subcontract; and
iv. total percentage of subcontractor(s) performance hours;
v. whether the subcontractor is affiliated with the bidder or has common ownership.

Please note the definition of "subcontractor" in the glossary in providing a proper response to this.

2. FACTORS USED TO EVALUATE CORPORATE OVERVIEW

Corporate Overview will be evaluated as follows:

i. the ability, capacity, and skill of the bidder to deliver and implement the system or project that meets the requirements of the Solicitation;
ii. the character, integrity, reputation, judgment, experience, and efficiency of the bidder;
iii. whether the bidder can perform the contract within the specified time frame;
iv. the bidder's historical or current performance; and

v. such other information that may be secured and that has a bearing on the decision to award the contract.

In evaluating the corporate overview, the Commission may consider: past experiences with the vendor; references; the Department of Administrative Services' record of the vendor, which may include, but is not limited to Vendor Compliance Request, Contract Non-Compliance Notice, or vendor performance reports; and any information related to the vendor's historical or current character, integrity, reputation, capability, or performance with the Commission, State or a third-party. Information obtained from any Contract Compliance Request or any Contract Non-Compliance Notice may be used in evaluating responses to determine the best value for the State.

3. RESPONSE TO SCOPE OF WORK

Bidder should read the Scope of Work Section of this RFP and provide a response as part of its proposal. This response should describe how the bidder will complete the scope of work, fill in any additional steps or details necessary, and demonstrate why the bidder is the most qualified or capable.

Additional Note: The response should not contain any reference to dollar amounts. However, information such as data concerning labor hours and categories, materials, subcontracts and so forth, may be considered so that the bidder's understanding of the scope of work may be evaluated.

4. RESPONSE TO WORK PLAN AND PROJECT PLANNING

Bidder should read the Work Plan and Project Planning Section of the RFP and provide a response as described in that section.

Additional Note: The response should not contain any reference to dollar amounts. However, information such as data concerning labor hours and categories, materials, subcontracts and so forth, may be considered so that the bidder's understanding of the scope of work may be evaluated.

5. RESPONSE TO TECHNICAL REQUIREMENTS

Bidder should read the Technical Requirements Section of the RFP and provide a response as described in that section. Appendix B contains a Technical Matrix to assist with compliance.

Additional Note: The response should not contain any reference to dollar amounts. However, information such as data concerning labor hours and categories, materials, subcontracts and so forth, may be considered so that the bidder's understanding of the scope of work may be evaluated.

6. COST PROPOSAL

Costs must be submitted as provided in the Cost Proposal (Appendix A). The Cost Proposal must include a complete response on all requested pricing information. Bidders may not take exception to any specific terms provided in the Cost Proposal.

The points awarded to a bidder will be determined by the following formula:

Points to Award = Lowest Bidder's Total Cost Submitted ÷ Bidder's Total Cost Submitted x Maximum Possible Points.

7. TERMS

Bidder should read the Terms provided with this RFP and must initial either "Accept All Terms and Conditions Within Section as Written" or "Exceptions Taken to Terms and Conditions Within Section as Written" in the table below (or include the same table in their solicitation response). If the bidder takes any exceptions, they must provide the following within the "Exceptions" field of the table; if an exception is not explicitly taken, it is deemed to be accepted as stated. The bidder may provide responses in separate attachment if multiple exceptions are taken. Exceptions must include:

1. The specific clause, including section reference, to which an exception has been taken;
2. An explanation of why the bidder took exception to the clause; and

3. Provide alternative language to the specific clause within the solicitation response.

Accept All Terms within Section as Written (initial)	Exceptions Taken to Terms Within Section as Written (Initial)	Exceptions: (Bidder must note the specific clause, including section reference, to which an exception has been taken, an explanation of why the bidder took exception to the clause, and provide alternative language to the specific clause within the solicitation response.)

The bidders should submit with their solicitation response any license, user agreement, service level agreement, or similar documents that the bidder wants incorporated in the Contract. The Commission will not consider incorporation of any document not submitted with the solicitation response as the document will not have been included in the evaluation process. These documents shall be subject to negotiation and will be incorporated if agreed to by the Parties.

8. CONTRACTUAL AGREEMENT FORM

The Contractual Agreement Form must be signed manually in ink, or by DocuSign or other electronic signature system, and returned by the opening date and time along with the bidder's solicitation. By signing the Contractual Agreement Form, the bidder guarantees compliance with the provisions stated in this solicitation and agrees to the terms and conditions unless otherwise indicated in writing.

B. FORMATTING AND PAGINATION

Pages in the Bidder's response may be consecutively numbered for the entire solicitation response or may be numbered consecutively within sections. Figures and tables should be numbered and referenced in the text by that number. They should be placed as close as possible to the referencing text.

C. PROPRIETARY INFORMATION

For any proprietary information contained in the solicitation response, the bidder should submit a detailed written document showing that the release of the proprietary information would give a business advantage to named business competitor(s) and explain how the named business competitor(s) will gain an actual business advantage by disclosure of information. The mere assertion that information is proprietary or that a speculative business advantage might be gained is not sufficient. (See Attorney General Opinion No. 92068, April 27, 1992). **THE BIDDER MAY NOT ASSERT THAT THE ENTIRE SOLICITATION IS PROPRIETARY. COST SHEETS WILL NOT BE CONSIDERED PROPRIETARY AND ARE A PUBLIC RECORD IN THE STATE OF NEBRASKA.**

The Commission will determine, in its sole discretion, if the disclosure of the information designated by the Bidder as proprietary would 1) give advantage to business competitors and 2) serve no public purpose. The Bidder will be notified of the Commission's decision. Absent a determination by the Commission that the information may be withheld pursuant to Neb. Rev. Stat. § 84-712.05, the Commission will consider all information a public record subject to disclosure. If the Commission determines it is required to release withheld proprietary information, the bidder will be informed. It will be the bidder's responsibility to defend the bidder's asserted interest in non-disclosure.

Glossary

The following definitions apply throughout the RFP, Scope of Work, and Terms.

99.999% (5 9s or 'Five Nines'): Requirement that the system be functional 99.999% of the time – equating to no more than 5.39 minutes of total downtime – planned or unplanned – each year. The Five Nines shall be applied to all systems, services, and operations and include the availability and reliability for the entire system.

911: A three-digit telephone number to facilitate the reporting of an emergency requiring response by a public safety agency.

911 Service Area: The geographic area that has been granted authority by a state or local governmental body to provide 911 service.

911 System: The set of network, database, and CPE components required to provide 911 services.

Abandoned Call: A call placed to 911 in which the caller disconnects before the call can be answered by the PSAP.

Acceptance: A manifestation of assent by the State to the Terms, Services, Deliverables, and/or other items offered by the Contractor under the Contract after inspection by the State.

Addendum: A written correction or alteration to a document during the solicitation process (e.g., Questions and Answers, Revised Schedule of Events, Addendum to Contract Award).

Additional Data: Describes the nature of how the call was placed, the person(s) associated with the device placing the call, or the location the call was placed from. Additional Data may include: "Additional Data for the Call," "Additional Data for the Caller," and "Additional Data for the Location."

Additional Data Repository (ADR): A data retrieval facility for Additional Data. The ADR dereferences a URI passed in a "Call-Info" header field or PIDF-LO <provided-by> and returns an Additional Data object block.

Advanced Encryption Standard (AES): FIPS-approved cryptographic algorithm that is used to protect electronic data.

Agency: An office, department, agency, institution of higher education, association, society, or other body in the State of Nebraska government created or authorized to be created by the State Constitution or any law, which is entitled to expend monies appropriated by law, including the legislature and the courts, but not including an authority, as defined in the State of Nebraska.

Agent: A person authorized to act on behalf of another.

Aggregation Point: The location of equipment to aggregate all traffic from a geographic area, region, or other defined location (normally POIs) to be merged (aggregated) prior to sending the entire bundle upstream. Aggregation points can reduce trunk costs by maximizing the network.

Alternate Routing: The capability of routing 911 calls to a designated alternate location(s) if all 911 trunks to a primary PSAP are busy or out of service. May be activated upon request or automatically, if detectable, when 911 equipment fails or the PSAP itself is disabled.

Amend: To alter or change by adding, subtracting, or substituting.

Amendment: A written correction or alteration to a document.

American National Standards Institute (ANSI): An entity that coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of US stakeholders in standardization forums across the globe.

Answering Position: The workstation at which 911 calls are answered and responded to by the Telecommunicator.

Application Programming Interface (API): A set of routines, protocols, and tools for building software applications. The API specifies how software components should interact, and APIs may be used when programming GUI components.

Applications and Appliances: The hardware and software required for 911 call and payload acceptance, processing, and delivery to a PSAP.

Appropriation: Legislative authorization to expend public funds for a specific purpose; money set apart for a specific use

Automatic Call Distributor/Distribution (ACD): The equipment that automatically distributed incoming calls to available PSAP Telecommunicators in the order the calls are received, or queues calls until a Telecommunicator becomes available.

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

Automatic Number Identification (ANI): A system which has the ability to automatically identify the caller's telephone number and provide a display at the CHE/CPE.

Award: All purchases, leases, or contracts which are based on competitive solicitations will be awarded according to the provisions in the solicitation.

Back-to-Back User Agent (B2BUA): A SIP element that relays signaling mechanisms while performing some alteration or modification of the messages that would otherwise not be permitted by a proxy server. A logical entity that receives a request and processes it as a UAS (user agent server). In order to determine how the request should be answered, it acts as a UAC (user agent client) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it establishes.

Baudot Code: A five-bit encoding scheme that represents text and digits. It is the standard transmission signaling scheme used by TDD and TTY devices. (EIA PN-1663)

Best and Final Offer (BAFO): In a competitive solicitation, the final offer submitted which contains vendor's most favorable terms for price.

Bid: See 'Solicitation Response'

Bid Opening: The process of opening correctly submitted solicitation responses at the time and place specified in the written solicitation and in the presence of any bidder who wishes to attend.

Bidder: A vendor who submits a Solicitation Response.

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

Border Gateway Protocol (BGP): A protocol designed to exchange routing and reachability information among autonomous systems.

Breach: Violation of a contractual obligation by failing to perform or repudiation of one's own promise.

Business: Any corporation, partnership, individual, sole proprietorship, joint-stock company, joint venture, or any other private legal entity

Business Day: Any weekday, except State-recognized holidays

Calendar Day: Every day shown on the calendar including Saturdays, Sundays, and State/Federal holidays

Call: A session established by signaling with two-way real-time media and involves a human making a request for help or a non-human initiated call. Sometimes it is referred to as a "voice call," "video call," or "text call" when specific media is of primary importance. The term "non-human-initiated call" refers to a one-time notification or series of data exchanges established by signaling with at most one-way media and typically does not involve a human at the "calling" end. The term "call" may also be used to refer to either a "Voice Call," "Video Call," "Text Call" or "Data-only Call," since they are handled the same way through most of Next Generation 911. It is an element of current and anticipated 911 payloads.

Call Delivery: The capability to route a 911 call to the designated selective router for delivery to the designated PSAP for the caller's ANI.

Call Detail Record (CDR): A record stored in a database recording the details of a received or transmitted call. The data information sent to the ALI computer by a remote identifying device (PBX, Call Position Identifier, etc.)

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

Call Identifier: A globally unique identifier assigned by the first element in the first ESInet which handles a call.

Call Processing: The system and process that permits a PSAP to receive, receive, process, and route a 911 call and other current and anticipated payloads to a PSAP within the defined environment providing complete payloads with callback and location information of the calling party to the call taker position. Call processing also includes the ability to identify and answer TDD/TTY and abandoned and silent calls including complete and accurate ANI and ALI of the TDD/TTY calls.

Call Queueing: The method of selection of which calls get passed to the outgoing trunk group when there are more call originations than terminating members on the outgoing trunk.

Call Relay: The forwarding of pertinent information by a PSAP Telecommunicator to the appropriate response agency.

Call Routing: The function of delivering the 911 call to the appropriate PSAP.

Call Transfer: The capability to redirect a call to another party.

Callback: The capability to re-contact the calling party.

Calling Party Hold: The capability of the PSAP to maintain control of a 911 caller's access line, even if the caller hangs up.

Cancellation: To call off or revoke a solicitation, purchase order, or contract without expectation of conducting or performing at a later time.

Carrier: A business entity that provides a function to a customer base, typically for a fee. Examples of carriers and associated services are a Local Exchange Carrier (LEC) providing PSTN service, a VoIP Service Provider providing VoIP service, and an Internet Service Provider providing email service.

Centralized Automated Message Accounting (CAMA): An MF signaling protocol originally designed for billing purposes, capable of transmitting a single telephone number.

Certificate Authority (CA): A trusted entity that issues digital certificates. The CA conducts a vetting process to ensure that the holder of the digital certificate is who they claim to be. Digital certificates are an essential part of secure communication and play an important part in the PKI.

Change Order: Document that provides amendments to an executed purchase order or contract.

Circuit: The physical path between two terminal locations.

Civic Address: Any city-style address that includes a house number and a street name is considered a Civic Address. Civic addresses include a community name that may or may not be recognized by the United States Postal Service or be MSAG valid. Civic addresses may be used as a Postal address if recognized by the United States Postal Service. Civic Addresses may be used as MSAG addresses if they are an exact match to the MSAG address. A rural route delivery address or FPO or APO address is not considered a Civic address.

Civic Location Data Exchange Format – United States (CLDXF-US): A United States profile of PIDF-LO that defines a set of standard data elements that describe detailed civic location information.

Collusion: An agreement or cooperation between two or more persons or entities to accomplish a fraudulent, deceitful, or unlawful purpose.

Communication Service Provider: An entity that provides communication services to a subscriber or end user.

Communication Services: Any of the following:

- (a) the transmission, conveyance or routing of real-time, two-way voice communications to a point or between or among points by or through any electronic, radio, satellite, cable, optical, microwave, wireline, wireless or other medium or method, regardless of the protocol used;
- (b) the ability to provide two-way voice communication on the public switched network;
- (c) wireless enhanced 911 service;
- (d) wireline enhanced 911 service;
- (e) interconnected VoIP provider service as defined by the regulations of the FCC regulations;
- (f) IP-enabled service; or
- (g) prepaid wireless service.

Competition: The effort or action of two or more commercial interests to obtain the same business from third parties

Computer-Aided Dispatch (CAD): A computer-based system which aids PSAP Telecommunicators by automating selected dispatching and record-keeping activities.

Confidential Data: Contractor's Confidential Information and the State's Confidential Information. Confidential Information shall not include information or material that:

- (a) is publicly available or becomes publicly available through no action or fault of the recipient party;
- (b) was already in the recipient party's possession or known to the recipient party prior to being disclosed or provided to the recipient party by or on behalf of the other party, provided, that, the source of such information or material was not bound by a contractual, legal or fiduciary obligation of confidentiality to the non-disclosing party or any other party with respect thereto;
- (c) was or is obtained by the recipient party from a third party, provided, that, such third party was not bound by a contractual, legal or fiduciary obligation of confidentiality to the non-disclosing party or any other party with respect to such information or material; or
- (d) is independently developed by the recipient party without reference to the Confidential Information.

See also 'Proprietary Information'

Contract: An agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law; the writing that sets forth such an agreement.

Contract Administration: The management of the contract which includes and is not limited to contract signing, contract amendments, and any necessary legal actions.

Contract Award: Document that officially awards a contract to a bidder(s) as the result of a competitive solicitation or a vendor(s) in a contract that qualifies for an exception or exemption from the competitive bidding requirements of the State Procurement Act.

Contract Management: The management of day-to-day activities at the agency which includes and is not limited to ensuring deliverables are received, specifications are met, handling meetings, and making payments to the vendor.

Contract Period: The duration of the contract.

Contractor: The entity entering into this Contract with the State.
See also 'Vendor'

Contractor's Confidential Information: Detailed information related to Contractor's network, infrastructure, and facilities the disclosure of which either:

- (a) could be used by hostile parties to attack those networks, infrastructure, and facilities, which are part of the nation's critical information infrastructure; or
- (b) negatively impact Contractor's competitive advantages by making information public that is not generally made available to Contractor's competitors.

Contractor's Confidential Information includes, but is not limited to, cybersecurity strategy, detailed network maps showing the location of nodes, facilities, conduit, and switches; detailed coverage maps; root causes analyses; and materials related to network monitoring and security. Contractor shall clearly mark such materials as confidential prior to disclosure to the State. For the sake of clarity, high-level conceptual diagrams showing network equipment and transport facilities without detailed location information (e.g., a stick diagram showing locations only with a city and state designation) are not sufficiently detailed to be Contractor's Confidential Information.

Copyright: A property right in an original work of authorship fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt and distribute the work

Cost Sheet: Commodities or Services specifically listed within the solicitation for evaluation

Critical Program Error: Any Program Error, whether or not known to the State, which prohibits or significantly impairs use of the Licensed Software as set forth in the documentation and intended in the contract

Customer Premises Equipment (CPE): Communications or terminal equipment located in the customer's facilities.
May also refer to Call Processing Equipment; See also 'Call Handling Equipment (CHE)'

Customer Service: The process of ensuring customer satisfaction by providing assistance and advice on those commodities or services provided by a vendor.

Cutover: The activation of a new telephone call processing or switching system.

Data Owner: The owner of information stored in the System as a Service solution.

Database: An organized collection of information, typically stored in computer systems, comprised of fields, records (data), and indexes. In 911, such databases include MSAG, telephone number/ESN, and telephone customer records.

Day: A calendar day unless otherwise specified in this RFP and subsequent contract.

Default: The omission or failure to perform a contractual duty, provide Deliverables, or render services as contractually required.

Default Routing: The capability to route a 911 call to a designated, default, PSAP when the incoming 911 call cannot be selectively routed due to an ANI failure or other cause.

Defense in Depth (DiD): Layered, overlapping controls that protect confidentiality, integrity, and availability across physical access, endpoints, data protection, boundary defenses, network and traffic separation, system monitoring, and (where applicable) vendor diversity.

Deliverable: Any work product or materials, which the contractor creates or delivers for the purposes of fulfilling its obligations to the State under the terms of the Agreement, including work products that the contractor must submit to the State for its approval in accordance with the formal acceptance procedures set forth in this RFP, and any planning documents, data, test or other documentation, diagrams, and schemas.

Deviation: Any proposed change(s) or alteration(s) to either the terms and conditions or deliverables within the scope of the written solicitation or contract

Discrepancies: A Service Provider term used to describe subscriber records that do not match the MSAG and are referred to an error file or report for resolution.

Domain Name System (DNS): The distributed "phone book" of the internet that translates human-readable names (e.g., nebraska.gov) into IP addresses so devices can find each other. Often used with UDP/TCP for queries and responses.

Domain Name System Security Extensions (DNSSEC): A set of DNS protocol extensions that use digital signatures to verify that DNS data is authentic and unaltered. DNSSEC adds a trust chain (signed zones and keys) so resolvers can detect spoofing and cache poisoning.

Electronic Industries Alliance (EIA): Developed standards to ensure that equipment of different manufacturers is compatible and interchangeable.

Element State (also ElementState): Term for the operational status of an i3 Functional Element; as 'ElementState' for use in the i3 schema, event packages, and log record names. [*Usage: "Update the Element State when a failover occurs and publish the ElementState event to the logging service."*]

Emergency Call: A request for public safety agency emergency services which requires immediate action to save a life, to report a fire, or to stop a crime. May include other situations as determined locally.

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

Emergency Incident Data Object (EIDO): A JSON-based object that is used to share emergency incident information between and among authorized entities and systems.

Emergency Service Number (ESN): A three- to five-digit number representing a unique combination of emergency service agencies (Law Enforcement, Fire, and Emergency Medical Service) designated to serve a specific range of addresses within a particular geographical area, or Emergency Service Zone (ESZ). The ESN facilitates selective routing and selective transfer, if required, to the appropriate PSAP and the dispatching of the proper service agency or agencies.

Emergency Services Internet Protocol Network (ESInet): 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 functional processes can be deployed, including, but not restricted to, those necessary for providing Next Generation 911 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).

Enhanced 911 (E911): An emergency telephone system which includes network switching, database, and CPE elements capable of providing Selective Routing, Selective Transfer, Fixed Transfer, ANI, and ALI.

Enhanced 911 Network Features: The components of enhanced 911 service that provide selective routing, ANI, and ALI.

Enhanced 911 Service: A service consisting of communication network, database and equipment features provided for subscribers or end users of communication services enabling such subscribers or end users to reach a PSAP by dialing the digits 911, or by other means approved by the department, that directs calls to appropriate PSAPs based on selective routing and provides the capability for ANI and ALI.

Enhanced 911 Service Provider: Any entity that provides one or more of the following 911 elements: network, database, or PSAP customer premises equipment.

Enhanced 911 System: A legacy 9-1-1 service that automatically delivers the caller's phone number and location (ANI/ALI) to the PSAP and routes the call to the correct PSAP via selective routing.

Evaluation: The process of examining a solicitation response after opening to determine the bidder's responsibility, responsiveness to requirements, and to ascertain other characteristics of the solicitation response that relate to determination of the successful award.

Evaluation Committee: Individual(s) identified by the agency that leads the solicitation to evaluate solicitation responses.

Extension: Continuance of a contract for a specified duration upon the agreement of the parties beyond the original Contract Period; not to be confused with "Renewal Period."

Federal Communications Commission (FCC): The federal agency that regulates communications by radio, television, wire, satellite, and cable across the United States.

Federal Information Processing Standards (FIPS): A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology (NIST), a part of the U.S. Department of Commerce. FIPS are a set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.

Five Nines: See '99.999%'

Foreign Corporation: A foreign corporation that was organized and chartered under the laws of another state, government, or country.

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

Functional Element (FE): A defined building block in the NENA i3 NG911 architecture that performs a specific function (logical role) and talks to other elements over standard interfaces. It may be software or hardware, centralized or distributed, and can be implemented by one or more vendors.

Geographic Information Systems (GIS): A computer software system that enables one to visualize geographic aspects of a body of data. It contains the ability to translate implicit geographic data (such as a civic address) into an explicit map location. It has the ability to query and analyze data in order to receive the results in the form of a map. It also can be used to graphically display coordinates on a map i.e., latitude/longitude from a wireless 911 call.

Graphical User Interface (GUI): The visual part of a software application that people click or tap to use it – windows, buttons, icons, menus, and screens – so users don't have to type commands.

Grievance: See 'Protest'

Host: A computer or other device connected to a computer network. A host may work as a server offering information resources, services, and applications to users or other hosts on the network. Hosts are assigned at least one network address.

HTTP Enabled Location Delivery (HELD): A protocol that can be used to acquire Location Information from a LIS within an access network as defined in RFC 5985.

i3: The NG911 system architecture defined by NENA, which standardizes the structure and design of Functional Elements making up the set of software services, databases, network elements, and interfaces needed to process multimedia emergency calls and data for NG911.

Identity Searchable Additional Data Repository (IS-ADR): An Additional Data Repository that provides a service that can search for Additional Data based on a sip/sips or tel URI (e.g., Additional Data about the caller).

Immediately Redirected: The instantaneous redirection of a 911 call to an alternative PSAP to prevent the loss of a 911 call.

Inspection: An examination of Deliverables or Services provided under this Contract to determine their fitness for use.

Instant Recall Recorder (IRR): A voice-band audio recorder which records to and plays from a media that may not be permanent (such as tape loop, fixed disk, or RAM). Recall recorders are typically associated with each operator position for the purpose of recording and playing back their most recent conversations. Also known as Call Check or Instant Playback Recorder.

Institute of Electrical and Electronics Engineers (IEEE): Promotes the development of standard and acts as a catalyst for new technology in all aspects of the engineering industry, including computer networking and telecommunications.

Integrated Services Digital Network (ISDN): A digital interface providing multiple channels for simultaneous functions between the network and CPE.

Interested Party: A person acting in their personal capacity or an entity entering into a contract or other agreement creating a legal interest therein

International Standards Organization (ISO): An independent, non-governmental international organization of national standards bodies.

Internet Engineering Task Force (IETF): The open, international standards body that develops and maintains internet protocols (e.g., TCP/IP, SIP, DNS). Work is done in public working groups and published as RFCs.

Internet Protocol (IP): The rules used to label and route data packets across networks, so they reach the right destination. IP provides addressing (IPv4/IPv6) and works with transport protocols like TCP and UDP.

Interoperability: The capability for disparate systems to work together.

IP-enabled Service: A service, device or application which makes use of IP and is capable of entering the digits 911, or by other means as approved by the department, for the purposes of interconnecting users to the NG911 systems including, but not limited to, VoIP and other services, devices, or applications provided through or using wireline, cable, wireless, or satellite facilities or any other facility that may be provided in the future.

JavaScript Object Notation (JSON): A lightweight data-interchange format based on a subset of the JavaScript Programming Language Standard ECMA-262.

Key Personnel: Specifically identified Contracted Personnel that play a lead and critical role in rendering Services during the Contract term.

Late Solicitation Response: A solicitation response received after the Opening Date and Time

Legacy Network: A 911 network that is operating as a basic or enhanced 911 system and/or the existing analog-based E911 systems in the State of Nebraska.

Legacy Network Gateway (LNG): A signaling and media interconnection appliance between analog callers in legacy wirelines/wireless originating networks and an i3 architecture so that PSAPs are able to receive emergency calls from such legacy networks.

Legacy PSAP: A PSAP that cannot process calls received via i3-defined call interfaces (IP-based calls) and still requires the use of CAMA or ISDN trunk technology for delivery of 911 emergency calls.

Legacy PSAP Gateway (LPG): An i3 functional element that supports the interconnection of the ESInet with legacy PSAPs.

Legacy Selective Router Gateway (LSRG): This gateway facilitates the routing/transfer of emergency calls between the ESInet and the legacy emergency services network. The LSRG will have to interwork location infrastructure between Next Generation 911 and legacy emergency services environments.

Location Information Server (LIS): A functional element that provides locations of endpoints. A LIS can provide Location-by-Reference, or Location-by-Value, and, if the latter, in geo or civic forms. A LIS can be queried for the location of an endpoint. In either case, the LIS receives a unique identifier that represents the endpoint, for example an IP address, circuit-ID, or MAC address, and returns the location (value or reference) associated with that identifier. The LIS also provides the dereferencing service, exchanging a location reference for a location value.

Location to Service Translation Protocol (LoST): A protocol that takes location information and a Service URN and returns a URI, is used generally for location-based call routing and, in Next Generation 911, is used as the protocol for the ECRF and LVF.

Location Validation: Refers to the action of ensuring that a civic address can be used to discern a route to a PSAP.

Location Validation Function (LVF): A function that provides sufficient location-based information to a PSAP that allows a 911 call taker to dispatch emergency responders to a 911 call scene. The location information is provided by civic based addresses or latitude/longitude data.

Logging Recorder: A voice-band audio recorder which records to and plays from a permanent storage media such as tape or disk. Logging recorders are typically multi-channel so as to simultaneously record from several sources.

Loopback: A type of diagnostic test in which a transmitted signal is returned to the transmitting device and then compared to the original signal.

Mandatory: Required, compulsory, or obligatory

Mapping Data Service (MDS): Provides a PSAP call taker with information showing the location of an out-of-area caller.

Master Street Address Guide (MSAG): A database of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 911 calls.

May: Discretionary, permitted; used to express possibility

Mean Time Between Failures (MTBF): The predicted elapsed time between inherent failures of a mechanical or electronic system during normal system operation. MTBF can be calculated as the arithmetic mean (average) time between failures of a system.

Mean Time to Repair (MTTR): The average amount of time it takes to repair or recover from an issue or failure in a system, equipment, or process.

Method of Procedure (MOP): A documented set of step-by-step instructions that outlines the specific actions and sequence of tasks required to complete a particular process or operation.

Millisecond (ms): One-thousandth of a second (0.001 s)

Multi-Frequency (MF): A type of signaling used on analog interoffice and 911 trunks.

Must: See 'Shall'

National Emergency Number Association (NENA): The National Emergency Number Association is a not-for-profit corporation established in 1982 to further the goal of "One Nation-One Number." NENA is a networking source and promotes research, planning and training. NENA strives to educate, set standards, and provide certification programs, legislative representation, and technical assistance for implementing and managing 911 systems.

Network Time Protocol (NTP): A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

Next Generation 911 (NG911): A Statewide emergency number system regardless of technology platform that does all of the following:

- (a) Provides standardized interfaces from requests for emergency assistance.
- (b) Processes all types of requests for emergency assistance, including calls and nonvoice and multimedia messages.
- (c) Acquires and integrates data useful to the delivery or routing and handling of requests for emergency assistance.
- (d) Delivers requests for emergency assistance and data to appropriate public safety answering points and emergency responders.
- (e) Supports data and communications needs for coordinated incident response and management.
- (f) Provides a secure environment for emergency communications.

Next Generation 911 System: The Next Generation 911 emergency communication SyaaS being procured via this RFP.
See also 'System as a Service (SyaaS)

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

No Record Found (NRF): A condition where no ALI information is available for display at the PSAP.

Nodes: In a communications network, a network node is a connection point that can receive, create, store, or send data along distributed network routes.

Non-Responsive Solicitation Response: Any solicitation response that does not comply with the requirements of the solicitation or cannot be evaluated against the other solicitation responses.

Nonnegotiable: These clauses are controlled by state law and are not subject to negotiation.

Open System Interconnection (OSI): Standardizes and explains how different computer systems communicate over a network.

Opening Date and Time: Specified date and time for the opening of received, labeled, and sealed formal solicitation responses.

Outsourcing: The contracting out of a business process that an organization may have previously performed internally or for which an organization has a new need to an independent organization from which the process is purchased back.

Overflow: The process of automatically rerouting calls to an alternate facility.

Payload: Any multi-media that presents to the network as a call, request for emergency assistance, or an equivalent, including without limitation, real-time communication and non-real time communication, voice, text, video, images, alerts, alarms, graphics, or telematics.

Performance Bond: An insurance agreement accompanied by a monetary commitment by which a third party (the surety) accepts liability and guarantees that the vendor fulfills any and all obligations under the contract.

Personally Identifiable Information (PII): An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if that element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable:

- (a) the individual's Social Security number;
- (b) the individual's driver's license number or state identification number;
- (c) the number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account;
- (d) the individual's DNA profile; or
- (e) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation, and any other information protected by state or federal law.

Plain Old Telephone Service (POTS): Legacy analog, circuit-switched telephone service delivered over copper pairs, providing basic dial tone and voice calling (and limited fax/modem use), typically powered from the central office – not IP-based.

Point of Contact (POC): The person designated to receive communications and to communicate

Point of Interconnection (POI): A Physical Demarcation between an originating carrier network and an NG911 network.

Point of Presence (PoP): The location at which one service provider exchanges traffic with another and provides interconnect services.

Presence Information Data Format (PIDF): Specified in IETF RFC 3863. It provides a common presence data format for Presence protocols and also defines a new media type. A presence protocol is a protocol for providing a presence service over the Internet or any IP network.

Presence Information Data Format – Location Object (PIDF-LO): An extension to PIDF that contains location information.

Preventative Maintenance: In general, tasks that are done to retain the healthy condition of equipment and prevent its failure.

Primary PSAP: A PSAP equipped with automatic number identification and automatic location identification displays and is the first point of reception of a 911 call. It serves the municipality in which it is located.

Prime Contractor: A general contractor that provides an aggregate of systems and components and assumes overall end to end responsibility for the Next Generation 911 system.

Private Branch Exchange (PBX): A private telephone system that is connected to the Public Switched Telephone Network.

Private Switch ALI (PS/ALI): A service operation which provides E911 features for telephone stations behind private switches (e.g., PBXs).

Project: The total scheme, program, or method worked out for the accomplishment of an objective, including all documentation, commodities, and goods to be provided under the contract

Proposal: See Solicitation Response

Proprietary Information: Trade secrets, academic and scientific research work that is in progress and unpublished or other information that if released would give advantage to business competitors and service no public purpose. See Neb. Rev. Stat. § 84-712.05(3). In accordance with Attorney General Opinions 92068 and 97033, proof that information is proprietary requires identification of specific named competitor(s) advantaged by release of the information and the demonstrated advantage the named competitor(s) would gain by the release of information.

Protest: A complaint about a governmental action or decision related to the solicitation or resultant contract under SPB's Protest Policy.

Pseudo Automatic Number Identification (pANI): A telephone number used to support routing of wireless 911 calls. It may identify a wireless cell, cell sector or PSAP to which the call should be routed. Also known as routing number.

Public Key Infrastructure (PKI): A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption.

Public Safety Agency: An entity that provides firefighting, law enforcement, emergency medical, or other emergency service.

Public Safety Answering Point (PSAP): A facility equipped and staffed to receive 911 calls. A Primary PSAP receives the calls directly. If the call is relayed or transferred, the next receiving PSAP is designated a Secondary PSAP.

Public Service Commission (PSC): Nebraska Public Service Commission

Public Switched Telephone Network (PSTN): The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.

Purchase Order (PO): The State's standard document of a purchase.

Quality of Service (QoS): A measurement of latency, packet loss, and jitter.

Queue State (also QueueState): Term for the current state of a call or media queue; as 'QueueState' for use in the i3 schema, event packages, or log record names related to queue status updates. Use when referring to identifiers, fields, or message types. [*Usage: "Publish a QueueState update when the Queue State changes (e.g., new wait-time estimate)."*]

QueueState Active: One or more entities are actively available or are currently handling calls being enqueued.

QueueState Disabled: The queue is disabled by management action, and no calls may be enqueued.

QueueState Full: The queue is full, and no new calls can be enqueued on it.

QueueState Inactive: No entity is available or actively handling calls being enqueued.

QueueState Standby: The queue has one or more entities that are available to take calls, but the queue is not presently in use. When a call is enqueued, the state changes to "Active."

Quote: See 'Solicitation Response'

Re-bid: A transaction initiated to collect accurate location information during a wireless call. Re-bid can be human initiated via a utility on the telecommunicator's screen or automatically as part of the system design.

Real-Time: The availability of information at the exact time it is occurring.

Redundancy: Duplication of components, running in parallel, to increase reliability.

Release Date: The date of public release of the solicitation

Remote Call Forwarding: As utilized within Interim Number Portability, a permanent call forwarding feature that allows a call to one Directory Number to be automatically advanced to a Directory Number of another Local Exchange Carrier.

Renewal Period: Optional contract periods subsequent to the original Contract Period for a specified duration with previously agreed to terms and conditions; not to be confused with "Extension"

Reorder Tone: An audible tone of 120 interrupts per minute (ipm) returned to the calling party to indicate the call cannot be processed through the network. Sometimes referred to as fast busy.

Repair: A permanent fix or repair, including replacement, if necessary, of a broken, damaged, or failed network device, database, or CPE that allows such system or system component to be fully operational.

Representative: See 'Agent'

Request for Proposal (RFP): See 'Solicitation'

Respondent: The company submitting a response to an RFP.

Response: A response from a Respondent to the RFP. A response may include submissions commonly referred to as 'bids,' 'quotes,' or 'proposals.'

Response Agency: The public safety agency having legal or consensual obligation to respond to a call for service.

Responsible Bidder: A vendor who has the capability in all respects to perform fully and lawfully all requirements with integrity and reliability to assure good faith performance.

Responsive Bidder: A vendor who has submitted a solicitation response which conforms to all requirements of the solicitation.

Ringback Tone: A tone returned to the caller to indicate that a call is being processed.

Root Cause Analysis (RCA): A report delivered after a disruption in the service provided by the SSP to explain, in detail, what the cause was, and what steps were taken to restore and recover normal operation.

Scope of Work: A subsection within the SOW that defines the boundaries – what's included and excluded, the objectives, and high-level requirements (often with explicit inclusions/exclusions).

Selective Routing: The routing of a 911 call to the proper PSAP based upon the location of the caller. The selective routing destination is determined by the ESN, derived from the caller's location.

Selective Transfer: The capability to transfer a 911 call to a response agency by operation of one of several buttons typically designated as police, fire, and emergency medical services; based on the ESN of the caller.

Service Level Agreement (SLA): A contract between a service provider and a customer that defines the service to be provided and the level of performance to be expected. An SLA also describes how performance will be measured and approved, and what happens if performance levels are not met.

Service Order: The Local Exchange Carrier document used for additions, changes, or removals of telephone service.

Service Provider: An entity providing one or more elements of an NG911 network.

Service State (also ServiceState): Term for a service's operational status (e.g., available, degraded, unavailable, maintenance, testing); as 'ServiceState' for use in the i3 schema, event packages, and log records. Use when referring to identifiers, fields, or message types. [*Usage: "When a service enters maintenance, update the Service State and publish a ServiceState event."*]

Session Initiation Protocol (SIP): A protocol specified by the IETF (RFC 3261) that defines a method for establishing multimedia sessions over the internet. Used as the call signaling protocol in VoIP, NENA i2 and NENA i3.

Shall: An order/command; mandatory

Should: Expected; suggested, but not necessarily mandatory

Signaling System 7 (SS7): An inter-office signaling network separate from the voice path network, utilizing high speed data transmission to accomplish call processing.

Single Point of Failure (SPoF): A component whose failure would stop the entire system or service from working.

Solicitation: A formal invitation to receive quotes in the form of a Request for Proposal or Invitation to Bid

Solicitation Bond: An insurance agreement, accompanied by a monetary commitment, by which a third party (the surety) accepts liability and guarantees that the vendor will not withdraw the solicitation response

Solicitation Conference: A meeting scheduled for the purpose of clarifying a written solicitation and related expectations

Solicitation Response: An offer, quote, bid, or proposal submitted by a vendor in response to a Solicitation

Source Database: The data base maintained by each Service Provider which provides customer telephone number and location information for the initial load and ongoing updates to the ALI database held by the Data Base Management System Provider.

Spatial Interface (SI): A standardized data replication interface used to publish GIS data to the functional elements that consume GIS data, such as the ECRF, LVF, Map Database Services, etc.

Specifications: The detailed statement, especially of the measurements, quality, materials, and functional characteristics, or other items to be provided under a contract

Standard Priority System Malfunction: Any trouble that is not defined as a Catastrophic System Malfunction, Major System Malfunction, or a High Priority System Malfunction.

State: Capitalized "State" means the State of Nebraska. Lower case "state" is to mean a state or condition within the operation of the network (e.g., the state of the functional element changed)

State's Confidential Information: All tangible and intangible information and materials being disclosed in connection with this Contract, in any form or medium without regard to whether the information is owned by the State or by a third party, which contains at least one of the following types of information:

- (a) Personally Identifiable Information;
- (b) Proprietary Information;
- (c) non-public information related to the State's employees, customers, technology (including data bases, data processing and communications networking systems), schematics, specifications, and all information or materials derived therefrom or based thereon;
- (d) information expressly designated as confidential in writing by the State; or
- (e)all information that is restricted or prohibited from disclosure by state or federal law.

Statement of Work (SOW): The contractual exhibit that spells out what will be done and how it will be managed – deliverables, tasks, milestones, schedule, acceptance criteria, roles, assumptions, and pricing terms.

Subcontract: An agreement, written or oral between the Contractor and any other party to fulfill the requirements and performance obligations of this Contract.

Subcontractor: Individual or entity with whom the vendor enters a contract to perform a portion of the work awarded to the vendor

Synchronization: In the context of timing, to bring clocks or data streams into phase so they agree with the PSAP master clock.

System as a Service (SyaaS): A turnkey offering in which the provider delivers, operates, secures, and supports the entire solution – hardware, software, network, hosting, monitoring, and updates – under defined SLAs.

System Service Provider (SSP): The entity acting as the prime 911 service provider for all calls and emergency traffic throughout the State – from caller to call-taker.

Telecommunications Device for the Deaf (TDD): Any type of text-based telecommunications equipment used by a person who does not have enough functional hearing to understand speech, even with amplification.

Telecommunicator: An emergency response coordination professional trained to receive, assess, and prioritize emergency requests for assistance, including, but not limited to:

- (a) Determining the location of the emergency being reported.
- (b) Determining the appropriate law enforcement, fire, emergency medical, or combination of those emergency services to respond to the emergency.
- (c) Coordinating the implementation of that emergency response to the location of the emergency.
- (d) Processing requests for assistance from emergency services.

Teletypewriter (TTY): A device capable of information interchange between compatible units using a dial up or private-line telephone network connections as the transmission medium. ASCII or Baudot codes are used by these units. (EIA PN 1663)

Termination: Occurs when either Party, under a power created by agreement or law, puts an end to the contract prior to the stated expiration date; all obligations that are still executory on both sides are discharged but any right based on prior breach or performance survives

Third-Party: Any person or entity, including but not limited to fiduciaries, shareholders, owners, officers, managers, employees, legally disinterested persons, and subcontractors or agents, and their employees. It shall not include any entity or person who is an interested party to the contract or agreement

Trade Secret: Information, including but not limited to, a drawing, formula, pattern, compilation, program, device, method, technique, code, or process that (a) derives independent economic value, actual or potential, from not being known to, and not being ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy (see Neb. Rev. Stat. § 87-502(4))

Trademark: A word, phrase, logo, or other graphic symbol used by a manufacturer or vendor to distinguish its product from those of others, registered with the U.S. Patent and Trademark Office

Transfer: A feature which allows the PSAP Telecommunicator to redirect a 911 call to another location.

Transmission Control Protocol (TCP): A connection-based transport protocol that delivers data in order and without loss. It sets up a session, checks for errors, resends missing pieces, and controls flow so neither side is overwhelmed.

Trouble: Any event that:

- impacts the functioning or operations of a PSAP; or
- is reported to the contractor's help desk by a PSAP or the State 911 Department.

Trouble Ticket: A tracking document that contains a concise, complete, and accurate history of the trouble from the time the trouble is reported to repair of the trouble. A trouble ticket shall include, but not be limited to, PSAP location, date and time of ticket opening, date and time of ticket closing, ticket number, detailed description of problem, all steps taken during repair efforts and reason for closing ticket.

Trunk: Typically, a communication path between Central Office switches, or between the 911 Control Office and the PSAP.

Trunk Group: One or more trunks terminated at the same two points.

Trunk Seizure: The point in time at which a 911 call is assigned to a trunk and acknowledgement is provided by the equipment at the distant end.

Underwriters Laboratories (UL): One of several nationally recognized testing laboratories whose testing specifications have been adopted as de facto industry standards.

Uniform Resource Identifier (URI): A predictable formatting of text used to identify a resource on a network.

Uniform Resource Name (URN): A URI that uses the URN schema and is intended to serve as persistent, location-independent resource names.

Uninterruptable Power Supply (UPS): An auxiliary power unit which provides continuous battery backup power in the event of a commercial power failure. Often used to bridge the power gap between commercial power interruption and the startup of standby generators – or, if needed, the controlled shutdown of critical equipment."

Universal Coordinated Time (UTC): It is a coordinated time scale, maintained by the Bureau International des Poids et Mesures (BIPM). It is also known as Zulu or Greenwich Mean Time (GMT). System logs should use UTC or local time with a UTC offset [Central Standard Time: UTC -6, Central Daylight Time: UTC -5].

Upgrade: Any change that improves or alters the basic function of a product of service

User Datagram Protocol (UDP): A connectionless transport protocol that sends small messages ("datagrams") without setup or guaranteed delivery. It's faster and lighter than TCP, often used for real-time voice, video, and DNS.

Vendor: An individual or entity lawfully conducting business with the State, or licensed to do so, who seeks to provide and contract for goods or services under the terms of a Solicitation and/or Contract.

Voice over Internet Protocol (VoIP): A type of IP-enabled service that allows for the two-way real time transmission of voice communications and has access to the public switched network.

Will: See Shall

Wireless Enhanced 911 Service: The service required to be provided by Wireless Carriers under, and governed by, FCC 96-264 and FCC 15-9.

Wireless Communications: The family of Telecommunications services under the heading of Commercial Mobile Radio Service. Includes Cellular, Personal Communications Services (PCS), Mobile Satellite Services (MSS) and Enhanced Specialized Mobile Radio (ESMR).

Wireline Carrier: A telephone service provider that delivers voice service over physical lines (copper or fiber), not wireless. This includes incumbent and competitive local exchange carriers (ILECs/CLECs) that provide access lines and interconnect to 911 networks.

Wireline Enhanced 911 Service: Legacy landline 9-1-1 service that routes calls via selective routers and delivers the caller's number (ANI) and service address record from the ALI/MSAG databases to the PSAP.

Work Day: See Business Day

Remainder of page intentionally blank

CONTRACTUAL AGREEMENT FORM

BIDDER MUST COMPLETE THE FOLLOWING

By signing this Contractual Agreement Form, the bidder guarantees compliance with the provisions stated in this solicitation and agrees to the terms and conditions unless otherwise indicated in writing.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603, DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Vendors. This information is for statistical purposes only and will not be considered for contract award purposes.

_____ NEBRASKA VENDOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Vendor. "Nebraska Vendor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this Solicitation. All vendors who are not a Nebraska Vendor are considered Foreign Vendors under Neb. Rev Stat § 73-603 (c).

_____ I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

_____ I hereby certify that I am a blind person licensed by the Commission for the Blind & Visually Impaired in accordance with Neb. Rev. Stat. § 71-8611 and wish to have preference considered in the award of this contract.

FORM MUST BE SIGNED MANUALLY IN INK OR BY DOCUSIGN

BIDDER:	
COMPLETE ADDRESS:	
TELEPHONE NUMBER:	
FAX NUMBER:	
DATE:	
SIGNATURE:	
TYPED NAME & TITLE OF SIGNER:	

Intent to Attend

Solicitation Conference

Solicitation Number 202691101

Bidder Name:	
Bidder Address:	
Contact Person:	
E-mail Address:	
Telephone Number:	
Fax Number:	
Number of Attendees:	

The “Intent to Attend Solicitation Conference” form should be uploaded using the ShareFile link provided in the SCHEDULE OF EVENTS