East Texas Council of Governments
3800 Stone Rd. Kilgore, TX 75662

REQUEST FOR QUALIFICATIONS: PS-911ESIN26R
9-1-1 ESInet 2026 RFP

David A. Cleveland, Executive Director, ETCOG

Stephanie Heffner, Director of Public Safety

RFP TIMELINE SCHEDULE (dates/times subject to change)

Bid Released	**Tuesday, November 10, 2026**
Questions Due	Monday, November 30, 2026
Staff Responses Post	Friday, December 4, 2026
Access Link Deadline	**Tuesday, February 2, 2027 11:00AM CST**
Bids Due	**Wednesday, February 3, 2027 11:00AM CST**

INTRODUCTION

East Texas Council of Governments

East Texas Council of Governments (ETCOG) is a voluntary association of counties, cities, school districts and special districts within a fourteen-county East Texas region. ETCOG assists local governments in planning for common needs, cooperating for mutual benefit and coordinating sound regional development. Either directly or through contractors, ETCOG provides programs and services for East Texas seniors, employers, and job seekers. ETCOG also builds the 9-1-1 emergency call delivery system, provides peace officer training and homeland security planning services; and delivers rural transportation services, business finance programs, grant writing services and environmental grant funding for the region.

PURPOSE

The East Texas Council of Governments (ETCOG) seeks submissions from qualified and experienced vendors in response to this Request for Proposal (RFP) issued for the purchase, migration, and implementation of a standards-compliant Next Generation 9-1-1 (NG9-1-1) Emergency Services Internet Protocol Network (ESInet) and Next Generation Core Services (NGCS).

PROPOSAL TERM

ETCOG intends to award a contract for an initial term of five (5) years, subject to the terms, conditions and performance requirements. The bid proposals and associated pricing provided in response to this RFP should be valid for a minimum period of 90 days, and preferably for a period of 180 days.

PROPOSAL REQUIREMENTS / SCOPE of WORK

ETCOG seeks to procure and implement an i3 standards-compliant regional Emergency Services Internet Protocol (IP) Network (ESInet) and Next Generation 9-1-1 Core Services (NGCS) that support transitional and end-state NG9-1-1 functionality. Procurement and implementation of these elements must recognize the need for interoperability with, and continuing support of, existing legacy systems currently in use. The ESInet will provide IP connectivity to every certified Public Safety Answering Point (PSAP) in the region and connectivity to interconnecting NG9-1-1 solutions operational in neighboring states and regional agencies. The NGCS will coordinate, manage and geo-route all 9-1-1 calls to appropriate 9-1-1 centers based upon the location of the caller and PSAP policies.

ETCOG seeks to realize this vision through the following objectives:

- Implementing an upgraded 9-1-1 system that will support NG9-1-1 call routing and data delivery using the latest available technology, and fully realizing ALL NG9-1-1 benefits.
- Evaluate and/or optimize systems, data, policies, procedures, and organizational structure to adequately support future needs regarding NG9-1-1 system operation.
- Plan, procure, and implement solutions that provide the greatest value to the agencies and citizens of the region.
- Carefully and strategically plan and execute necessary organizational and technical objectives with minimal disruptions to stakeholders.

The ETCOG ESInet/NGCS anticipates providing services to all 19 PSAPs and 2 host sites in the ETCOG service area. While all are anticipated to interconnect with the ETCOG's ESInet/NGCS, they are at differing levels of i3 readiness, with some requiring the transitional functions described in NENA-STA-010.3f-2021 and NENA-STA-034.1-2022 for an undisclosed period of time. Included in an attachment to this RFP is statistical/logistical information that is critical for the respondent to consider, including total seats and seats per PSAP, primary/backup classifications, year over year incoming 9-1-1 call totals, and PSAP primary/backup locations. ETCOG's PSAPs today consist of host-remote deployments.

ETCOG offers no preference as to the physical location of the "service"— cloud-based or premises-based — but rather seeks the best value for compliance to the technical requirements necessary to support the required functionality.

Company Description

Respondent will include a brief description of company background, including history, experience, products, capabilities, and vision for the future, as well as any distinguishing characteristics that differentiate their solution from other companies' solutions.

Respondent's description must include the following information with the proposal response:

a. Background and experience
b. Company vision
c. Company financial stability statement
d. Distinguishing solution characteristics
e. Pending litigation
f. Identification of the number of ESInet/NGCS solutions, comparable to the one being proposed for ETCOG, that have been installed and are currently operational
g. References (at least three that demonstrate similar implementation of the service model solution proposal). The Respondent is required to complete the forms included in the *Current References* section of this RFP.
h. Details describing how your company provides Service Maintenance and after-sales service support.

☐ Understood

Interoperability

To ensure interoperability among all components of the ESInet/NGCS solution and planned or deployed i3 CHE solution(s), all Respondents must commit to, and document (prior to completion of contract negotiation), interoperability with available i3 CHE solutions. Respondent(s) must identify all of the CHE solutions with which their solution currently operates, and describe the mechanisms used to assess this interoperability. Supporting documentation of interoperability is desirable and may take the form of references from customers where solutions have been deployed and made operational for a minimum of six months. Respondents should also identify any CHE with which their ESInet/NGCS solution is not compatible, explain the reasons for any incompatibility with specific CHE solutions, and describe any plans or possibilities for future compatibility.

To ensure interoperability between components of the proposed ESInet/NGCS solution and other ESInet/NGCS solution(s), all Respondents must commit to, and document (prior to completion of contract negotiation), interoperability with available ESInet/NGCS solutions and identify whether this interoperability uses i3-compliant Network-to-Network Interfaces (NNIs). Respondent(s)

must identify all of the ESInet/NGCS solutions with which their solution currently operates.

In support of the rules outlined in the Federal Communications Commission Report and Order in the Matter of Facilitating Implementation of Next Generation 911 Services (NG911)[1], the proposed solution must support ETCOG in certifying that it is technically ready to receive 9-1-1 calls and texts in the IP-based format requested. In addition, the Respondent must commit to facilitating and completing connectivity testing with Originating Service Providers (OSPs) within the compliance timeframe applicable to the OSP.

ETCOG will work with the Respondent to identify Points of Interconnection (POIs) associated with other networks that the Respondent's ESInet/NGCS will interconnect with, including other ESInets within and outside of the region, and interconnection with Originating Service Provider (OSP) networks. POIs supporting the interconnection of the Respondent's ESInet/NGCS with OSP networks must align with the rules outlined in the Federal Communications Commission Report and Order in the Matter of Facilitating Implementation of Next Generation 911 Services (NG911).

☐ Understood

Industry Standards

ETCOG seeks a standards-based solution that complies with nationally accepted standards and requirements applicable to IP network architecture, security, and interface functionality. All aspects of the Respondent's proposed system design, deployment, operation, and security shall be in full compliance with the standards, requirements, and recommendations identified in the following documents. The relevant Standards Development Organizations (SDOs) include:

- Association of Public-Safety Communications Officials (APCO)
- National Emergency Number Association (NENA)
- Alliance for Telecommunications Industry Solutions (ATIS)
- Department of Justice (DOJ)
- Internet Engineering Task Force (IETF)
- National Institute of Standards and Technology (NIST)
- Telecommunications Industry Association (TIA)
- The Monitoring Association (TMA) (formerly known as the Central Station Alarm Association [CSAA])

[1] FCC 24-178 Facilitating Implementation of Next Generation 911 Services (NG911) - https://www.fcc.gov/document/fcc-takes-action-expedite-transition-next-generation-911-0

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
APCO/TMA	2.101.3-2021	Alarm Monitoring Company to Emergency Communications Center (ECC) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)	Provides detailed information on data elements and structure standards for electronic transmission of new alarm events from an alarm monitoring company to an ECC.	Version 3.4 2021
APCO/ NENA	1.102.3.2020	Emergency Communications Center (ECC) Service Capability Criteria Rating Scale	APCO and NENA jointly have developed an assessment tool to evaluate current capabilities of the ECC against models representing the best level of preparedness, survivability, and sustainability amidst a wide range of natural and manmade events.	Version 3 2020
ATIS/TIA	ATIS J-STD-110.v002	Joint ATIS/TIA Native SMS/MMS Text To 9-1-1 Requirements and Architecture Specification	The purpose of this Standard is to define the requirements, architecture, and procedures for text messaging to 9- 1-1 emergency services using native Commercial Mobile Service Provider (CMSP) Short Message Service (SMS) or Multimedia Message Service (MMS) capabilities for the existing generation and next	Release 2 May 1, 2015

[2] For any standards, if a newer version is available at the time of publication of this RFP, compliance will be judged relative to the latest version.

			generation (NG9-1-1) Public Safety Answering Points (PSAPs).	
ATIS	ATIS-0700015.v006	ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination	Provides standards addressing communications originating from an IP Multimedia Subsystem (IMS) subscriber and delivered to a National Emergency Number Association (NENA) i3 Emergency Services IP network (i3 ESInet) and associated NG9-1-1 Core Services (NGCS), or to a legacy Selective Router	Version 6 February 2026
ATIS	ATIS-1000074.v003	Signature-based Handling of Asserted information using toKENs (SHAKEN)	This document provides telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies to validate legitimate calls and mitigate illegitimate spoofing of telephone identities on IP-based service provider voice networks	Version 3 August 2022
U.S. Department of Justice	CJISD-ITS-DOC-08140-6.0	Criminal Justice Information Services (CJIS) Security Policy	Provides information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information	Version 6.0 December 27, 2024

IETF	RFC 3261	SIP: Session Initiation Protocol	Describes the SIP, an application-layer control (signaling) protocol for creating, modifying, and terminating sessions (including Internet telephone calls, multimedia distribution, and multimedia conferences) with one or more participants	June 2002
IETF	RFC 4103	RTP Payload for Text Conversation	Describes how to carry real-time text conversation session contents in Real-time Transport Protocol (RTP) packets	June 2005
IETF	RFC 4119	A Presence-based GEOPRIV Location Object Format	Describes an object format for carrying geographical information on the Internet.	December 2005
IETF	RFC 4579	Session Initiation Protocol Call Control - Conferencing for User Agents	Defines conferencing call control features for the Session Initiation Protocol (SIP).	August 2006
IETF	RFC 5222	LoST: A Location-to-Service Translation Protocol	Describes a protocol for mapping service identifiers and geodetic or civic location information to service contact URIs	August 2008
IETF	RFC 5491	GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations	Provides recommendations on how to constrain, represent, and interpret locations in a PIDF-LO	March 2009
IETF	RFC 6442	Session Initiation Protocol Location Conveyance	Defines an extension to the Session Initiation Protocol (SIP) to convey	December 2011

			geographic location information from one SIP entity to another SIP entity	
IETF	RFC 6753	A Location Dereferencing Protocol Using HTTP-Enabled Location Delivery (HELD)	Describes how to use the Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) as a dereference protocol to resolve a reference to a Presence Information Data Format Location Object (PIDF-LO)	October 2012
IETF	RFC 6874	Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers	Extends RFC 3986 to allow a zone identifier to be included in an IPv6 address	February 2013
IETF	RFC 7852	Additional Data Related to an Emergency Call	Describes data structures and mechanisms to convey information about an emergency call, caller, or location to the PSAP by value or by reference	July 2016
IETF	RFC 7090	Public Safety Answering Point (PSAP) Callback	Describes a mechanism for marking PSAP callbacks using a new header field value for the SIP Priority header field, called "psap-callback"	April 2014
IETF	RFC 8224	Authenticated Identity Management in the Session Initiation Protocol (SIP)	This document defines a mechanism for securely identifying originators of SIP requests	February 2018
IETF	RFC 8865	T.140 Real-Time Text Conversation over WebRTC Data Channels	Specifies how a Web Real-Time Communication (WebRTC) data channel can be used as a transport mechanism	January 2021

			for real-time text.	
NENA	NENA-REQ-001.1.2-2018	NENA Next Generation 9-1-1 Public Safety Answering Point Requirements	Provides requirements for functions and interfaces between an i3 PSAP and NGCS, and among functional elements associated with an i3 PSAP	Version 1.1.2 June 10, 2018
NENA	NENA-STA-006.3-2026	Standard Data Formats for 9-1-1 GIS Data Model	This document defines the GIS data information, formats, requirements and related information used in NENA Next Generation 9-1-1 (NG9-1-1) Core Services (NGCS)	Version 3 March 11, 2026
NENA	NENA-STA-008.2-2014 (originally 70-001)	Registry System Standard	Describes how registries (lists of values used in NG9-1-1 functional element standards) are created and maintained	Version 2 October 6, 2014
NENA	NENA-STA-010.3f-2021	NENA i3 Standard for Next Generation 9-1-1	Builds upon prior NENA publications including i3 requirements and architecture documents and provides additional detail on functional standards	Version 3f December 17, 2024
NENA	NENA-STA-015.10.1-2026	NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping	Provides standard formats for Automatic Location Identification (ALI) data exchange between Service Providers and Data Base Management System Providers	Version 10.1 March 24, 2026
NENA	NENA-STA-018.2-2021 (originally 05-001)	NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2	This document clarifies the E2 interface defined in J-STD-036 and defines the content of parameters that are not fully defined therein	Version 2 February 17, 2021

NENA	NENA-INF-016.2-2018 (formerly 08-506)	Emergency Services IP Network Design Information Document (ESIND) for NG9-1-1	Provides information that will assist in developing the requirements for and/or designing an i3-compliant ESInet	Version 2 April 5, 2018
NENA	NENA 54-750	NENA/APCO Human Machine Interface & PSAP Display Requirements (ORD)	Prescribes requirements for the human machine interface (HMI) display for the Next Generation 9-1-1 (NG9- 1-1) System	Version 1 October 20, 2010
NENA	NENA-STA-040.2-2024	NENA Security for Next Generation 9-1-1 (NG-SEC)	Establishes the minimal guidelines and requirements for levels of security applicable to NG9-1-1 entities	November 4, 2024
NENA	NENA-REF-012.1-2025	Security Audit Checklist	This document is a companion to NENA-STA-040.2-2024 NENA Security for Next Generation 9-1-1 Standard (NG-SEC) and is used to assess compliance with requirements specified in NENA-STA-040.2-2024	May 6, 2025
NENA	NENA-INF-008.2-2013 (previously NENA 77-501)	NENA NG9-1-1 Transition Plan Considerations Information Document	Provides NENA's recommendations for transitioning to NG9-1-1	November 20, 2013
NENA	NENA-INF-015.1-2016	NG9-1-1 Security (NG-SEC) Information Document	Provides mechanisms and best practices for cybersecurity for i3 systems	Version 1 December 8, 2016
NENA	NENA-INF-040.2-2022	NENA Managing & Monitoring NG9-1-1 Information Document	Provides guidance on best practices for monitoring and managing NG9-1-1 services and infrastructure.	Version 2 July 27, 2022
NENA	NENA-STA-021.1b-2022	NENA Standard for Emergency Incident	Provides standard format for exchanging emergency	Version 1b December

		Data Object (EIDO)	incident data between disparate systems and agencies	17, 2024
NENA	NENA-STA-024.1.1-2025	NENA Standard for the Conveyance of Emergency Incident Data Objects (EIDOs) between Next Generation (NG9-1-1) Systems and Applications	Defines how EIDOs are conveyed between Functional Elements	Version 1.1 January 30, 2025
NENA	NENA STA-031.1-2021	NENA Standard for Interconnecting Emergency Services IP Networks and Public Safety Broadband Networks	Establish standards for interconnections between ESInets and other broadband networks used by first responders.	October 14, 2021
NENA	NENA-STA-034.1-2022	NENA Legacy Selective Router Gateway (LSRG) Standard	Provides a technical standard for the LSRG which is a signaling and media connection point between a legacy Selective Router and an i3 ESInet/NGCS	March 17, 2022
NENA / NIOC	NG9-1-1 PKI VP V1.0	NG9-1-1 Interoperability Oversight Commission (NIOC) (PSAP) Credentialing Authority (PCA) Certification Validation Guidelines	Provides the security requirements needed to support the secure validation for issuance of Certificates in NG9-1-1 by the PCA Certification Authorities (CAs) in the NG9-1-1 Public Key Infrastructure.	V1.0.0 February 9, 2022
NENA / NIOC	NG9-1-1 PKI CP v1.2	Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy	Provides the security requirements needed to support the secure issuance of Certificates in NG9-1-1 by the PCA CAs in the NG9-1-1 Public Key Infrastructure.	V1.2 June 26, 2024
NIST	FIPS 140-3	Security	Specifies security	Version 2

		Requirements for Cryptographic Modules	requirements that will be satisfied by a cryptographic module utilized with a security system protecting sensitive but unclassified information	March 22, 2019
NIST	Cybersecurity Framework 2.0	The NIST Cybersecurity Framework (CSF) 2.0	Provides standards, guidelines, and best practices that promote the protection of critical infrastructure	Version 2.0 February 26, 2024
TIA	TIA-942-B	Telecommunications Infrastructure Standard for Data Centers	Specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms, including single-tenant enterprise data centers and multi-tenant Internet-hosting data centers	Revision B July 12, 2017

Table 1: Adopted Standards

As industry standards evolve, the Respondent's solution shall be upgraded to maintain compliance with the current version of established industry standards. The Respondent's solution shall support new IP network, security, and NG9-1-1 industry standards within 18 months of ratification of the applicable industry standards. If the Respondent is not compliant with the version or revision listed, we ask that they identify their compliant version. Compliance requirements apply also to the supporting standards referenced within each standard. As solution updates are made to maintain compliance, the solution shall not abandon services or feature functionality in place at the time of the solution upgrade. The Respondent shall divulge any performance or feature changes uncovered prior to the upgrade and report them to ETCOG for approval. The Respondent shall advise ETCOG of scheduled upgrades and discuss costs to ETCOG, if any, before deployment of upgrades.

☐ Understood

TECHNICAL QUALIFICATIONS

This *Technical Qualifications* section is comprised of a series of tables. Each table contains specific requirements, applicable to a particular aspect of the associated solution, as indicated by the heading immediately preceding each table. The Respondent is required to clearly mark one (and only one) of the three right-most columns (Complies, Does Not Comply, Partially Complies) for each requirement, as follows:

- **Complies** – The proposed solution does, today (or will, at the time of contract award), fully satisfy the requirement.
- **Does Not Comply** – The proposed solution does not, today (nor will it, at the time of contract award), substantially satisfy the requirement.
- **Partially Complies** – The proposed solution does, today (or will, at the time of contract award), substantially (though incompletely or, perhaps, in an alternate way) satisfy the requirement.

Following each table is a space for the Respondent to add additional information that supports, or elaborates upon, the compliance declaration for the requirements in the table. Respondents must provide a response and detailed description for each requirement.

☐ By checking this box, you acknowledge you have read and understand.

ESInet

Respondent's ESInet solution must comply with the following	Complies	Does Not Comply	Partially Complies
1. Has redundant ESInet connectivity to each CHE core or host site.			
2. Has diverse entrance facilities for call handling host and ETCOG-selected standalone call answering points			
3. Has no single points of failure, including "last mile" To ensure the most robust and reliable network architecture possible, please describe your ESInet diversity strategy, including the number and types of connections (including the use of different technologies such as			

wireless, satellite, microwave), and the number of providers involved in supporting diversity in your ESInet solution. (See the *Documentation* section of this RFP, Item #6 for requirements related to documentation of network design details.)			
4. Uses open standards			
5. Supports new IP network, security, and NG9-1-1 industry standards within 18 months of ratification of applicable industry standards			
6. Supports IPv4 and iPv6 dual protocol stacks			
7. Supports Border Gateway Protocol (BGP) utilizing Bidirectional Forwarding Detection			
8. Supports multicast routing and switching			
9. Supports quality of service (QoS) marking using Differentiated Service Code Point (DSCP)			
10. Has a network traffic convergence of less than 54 milliseconds (ms)			
11. Maintains a Mean Opinion Score (MOS) of 4.0 or better at the handoff to the call handling equipment			
12. Is scalable to support bandwidth growth by 50 percent			
13. Shall interface with ETCOG-selected other i3-compliant ESInets to facilitate ESInet-to-ESInet routing/transfers over fully functional i3 NNIs, conveying standard data			
14. Provides redundant in-state IP POIs[3] for Originating Service Provider interconnection. Please specify the location of these POIs.			
15. Failure of any single instance of a hardware or software element, or physical connection (except ETCOG-designated single connection PSAPs), shall not negatively impact overall solution performance			
16. All network-connected elements must support at least two redundant and physically diverse network interfaces			

[3] Points of Interconnection.

17. All powered devices must include a minimum of two redundant power supplies (each of which must be able to power the device, alone, and which would be connected to separate circuits) OR be connected to a power-transfer device that allows a single power supply to be connected to two isolated power sources (i.e., circuits) with automatic, uninterrupted failover, in the event the primary circuit fails			
18. All SIP elements must support Transport Layer Security (TLS), Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) transport. SIP signaling within the ESInet should utilize TLS where available. If TLS transport fails or is not available, SIP elements in the ESInet should attempt to use TCP. If TLS and TCP transports both fail or are unavailable, SIP elements should fall back to UDP transport.			
19. Connections between the ESInet and the PSAP shall support TCP/IP connections with Transport Layer Security.			
20. The ESInet shall be engineered to sustain real-time traffic, including data, audio, and video.			
21. The ESInet must provide a Network Time Protocol (NTP) service for time-of-day information via a hardware clock, or synchronization to another NTP time service. Time accuracy must be within 1 ms of true time.			
22. The Respondent's proposed ESInet solution must be interoperable with other interconnecting ESInets, as identified by ETCOG a. Please identify all of the ESInet/NGCS solutions with which your solution currently operates, and indicate whether the interconnection utilizes a fully functional i3 NNI. b. Describe in detail any additional costs associated with inter-ESInet connectivity (e.g., circuit costs), beyond the cost of the proposed solution, including the basis (e.g., per circuit, per PSAP) and frequency (e.g., monthly recurring, one-time/non-recurring) of the associated charges			

23. Coordinate and execute connectivity to neighboring ESInets to support transfers to neighboring agencies not served by ETCOG's NG9-1-1 solution, including bridging functionality and conveyance of call/incident information (i.e., Emergency Incident Data Objects [EIDOs])			
24. The Respondent shall identify all the CHE solutions with which their solution currently operates, and specifically whether the solution interoperates with Vesta CHE currently deployed in the ETCOG region.			

Details to support the response: Please indicate the bandwidth supported by your architecture and describe how the proposed bandwidth is sufficient to support voice, video, imagery, and text communications. Describe your strategy for supporting bandwidth growth. Please specify the Data Transmission Rate (DTR) supported by your architecture. Please identify whether you have participated in any NENA Industry Collaboration Event (ICE) activities, and if so, which one(s).

Security

Respondent shall:	Complies	Does Not Comply	Partially Complies
1. Provide a completed Security Audit Checklist (see NENA-REF-012.2-2025)			
2. Have a security plan (physical, logical, and network)			
3. Perform proactive analysis of the network for vulnerabilities			
4. Have a documented Risk Management process, including the use of a standard framework (e.g., NIST Cybersecurity Framework) for identifying and mitigating threats such as Telephony Denial of Service (TDoS) and Distributed Denial of Service (DDoS) attacks, malware, session hijacking, credential reuse, etc.			

Respondent shall:	Complies	Does Not Comply	Partially Complies
5. Conduct a security assessment (internal or external), at a minimum, annually; conduct an external assessment at a minimum, once every 3 years			
6. Provide a defined Cybersecurity Incident Response Policy defining procedures and actions to take in the event of a cybersecurity incident as well as how and when to bring in outside assistance			
7. Control all physical access points (except for those areas within the facility officially designated as publicly accessible) and verify individual access authorizations before granting access			
8. Provide access reports from facilities down to the individual device level			
9. Require multifactor authentication (MFA) for any access to externally accessible portals, user interfaces (UIs), etc. (Policy Routing Function portal, reporting portal, system dashboards, etc.)			
10. Require new devices and applications that have local accounts to have a new password set in accordance with the Authentication/Password policy for each local account prior to being connected to any system/network. Password security policies should include, for example, the use of strong passwords and password expiry/change timeframes. (See CISA guidelines regarding strong passwords.)			
11. Provide an infrastructure that is built to withstand TDoS and DDoS attacks			
12. Support the application of SHAKEN caller identity authentication/verification procedures as specified in NENA-STA-010.3f, *NENA i3 Standard for Next Generation 9-1-1.*			

Respondent shall:	Complies	Does Not Comply	Partially Complies
13. Provide a Data Security Policy that defines the data classification levels, how that data is to be labeled, handled, stored, managed, and disposed of.			
a. Protection of Sensitive Data at rest shall be defined in the Data Protection Policy. Data that contains confidential information must be stored encrypted, using Advanced Encryption Standard (AES) with a minimum key length of 256 bits (AES 256) or an equivalently strong algorithm.			
b. Sensitive Data in transit requires end to end encryption and shall be defined in the Data Protection Policy. This applies to all internal and external networks that the Sensitive Data traverses. All protocol operations must be privacy-protected via TLS, preferably using AES 256.			
14. Support access control for Agents (e.g., to support access to the Authorization and Data Rights Management mechanism described in NENA-STA-010.3f) implemented using a universal Single Sign On (SSO) paradigm using OASIS SAML (Security Assertion Markup Language).			
15. Limit storage of data associated with a cloud-hosted solution to be within the United States			
16. To help mitigate the impacts from cyberattacks, utilize the 3-2-1 backup strategy described in *Data Backup Options*[4]. This entails having three (3) backups on two (2) different forms of media storage (such as cloud, tape, external drive, flash drive) that can be connected on demand, and store one (1) copy offsite.			

[4] US-CERT, Data Backup Options, https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf.

Respondent shall:	Complies	Does Not Comply	Partially Complies
17. Provide valid backups and support at least quarterly testing of those backups to ensure the ability to recover from those backups. Backed up information should include system images, server images, configuration files, data, data bases, log files, licensing, software, and any required data			

Details to support the response: Please describe the mechanism that your solution uses to support multifactor authentication.

Facilities

Respondent facilities (i.e., Data Centers, Points of Interconnection, hosting sites, clouds, etc. outside of the PSAP where Respondent-provided equipment is used to deliver the contracted Services) shall comply with the following:	Complies	Does Not Comply	Partially Complies
1. All power sources must be redundant and diverse (i.e., at least two separate circuits) with an Uninterruptible Power Supply (UPS) system and generator backup for a minimum of 24 hours			
2. Deliver voice and data circuits via diverse entrances into facilities			
3. Deliver voice and data circuits from diverse providers			
4. Secured rack space			
5. Minimum Tier 3 rated			
6. Hardened facilities that can withstand EF5-category winds up to 318 miles per hour			
7. Must properly flag emergency services circuits			

Details to support the response:

Monitoring and Alarming

Respondent shall provide the following monitoring and alarming capabilities:	Complies	Does Not Comply	Partially Complies
1. Physical access monitoring and reporting			
2. Automated real-time network node monitoring and alarming			
3. Integrated alarming and ticketing system			
4. Ability to display network node status in a client-facing dashboard			
5. User-definable notification levels and recipients, with text and email delivery options			
6. Support for *Best Practice Thresholds for Monitoring NG9-1-1 Functional Elements*, as specified in NENA-INF-040.2			

Details to support the response:

Service Continuity

Respondent shall provide the following service continuity measures:	Complies	Does Not Comply	Partially Complies
1. Provide a defined continuity of operations plan (COOP) as well as a disaster recovery (DR) plan			
2. Have a formal change management/control process documented with rollback procedure and management approvals that is strictly followed by technicians (to prevent unnecessary and/or uncontrolled maintenance from negatively impacting the 9-1-1 system)			

Details to support the response:

NOC/SOC

Respondent shall provide the following NOC/SOC[5] capabilities:	Complies	Does Not Comply	Partially Complies
1. 24 x 7 x 365 staffed NOC/SOC to support continuous monitoring, review, and analysis of network and security activity			
2. Ability for users to submit tickets by phone, and direct ITSM[6] user access for incidents, problems, and changes			
3. Perform outward notifications and updates of customer tickets through phone, email, and text			
4. Support interactions between ETCOG and technical support personnel via collaborative tools, such as Zoom, Google Meet, Microsoft Teams, Webex.			
5. Have an executive dashboard with (near) real-time updates of tickets and network status			
6. Comply with SLAs for notification and ticket resolution as outlined in Table 5 *Service Level Requirements, Metrics, and Remedies* of this RFP			
7. Reason For Outage (RFO) reports and regulatory compliance according to Federal Communications Commission (FCC) standards. *Note that the FCC defines an "outage" as "a significant degradation in the ability of an end user to establish and maintain a channel of communications as a result of failure or degradation in the performance of a communications provider's network."*			
8. Preliminary RFO reports are due to ETCOG within 1 business day; final root-cause analysis within 15 business days			
9. Immediate point of contact for any outage or service failure. Note that the Respondent is responsible for keeping the contact list up-to-date.			
10. Government and regulatory contact for any outage or service failure			

[5] Network Operations Center/Security Operations Center.
[6] IT Service Management.

Respondent shall provide the following NOC/SOC[5] capabilities:	Complies	Does Not Comply	Partially Complies
11. Access to technical staff for escalations			
12. Compliance with Statement on Standards for Attestation Engagements Number 18 (SSAE 18)			
13. Support of eBonding in the ITSM platform			
14. Support for third-party monitoring (e.g., via integration with a third-party NOC/SOC)			
15. Have established escalation procedures			
16. All NOC/SOC access is US-based; no “offshore” remote access into systems installed within the ETCOG network for general system administration, maintenance, or troubleshooting			
17. All remote access into systems installed within the ETCOG network for general administration, maintenance, or troubleshooting shall be logged			

Details to support the response:
Explain if your NOC/SOC is owned or outsourced, and if outsourced, identify where and to whom it is outsourced.

Next Generation Core Services – NGCS Functional Elements

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
1. Border Control Function (BCF), that supports the following functionality, as described in NENA-STA-010.3f-2021			
a. Session Border Control functionality including:			
i. Identification of emergency call/sessions and priority handling of emergency call/session traffic			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
ii. Conformance checking and mapping (if applicable) of QoS/Priority Packet Markings based on policy for emergency calls/sessions			
iii. Adding Call and Incident Tracking identifiers to the signaling			
iv. Adding the Resource-Priority header field if not already included			
v. Policing Resource-Priority header value			
vi. Protection against DDoS attacks			
vii. SIP Protocol Normalization			
viii. IPv4/IPv6 Interworking			
ix. IP payload processing/transcoding			
x. Media protection			
xi. Back-to-back user agent (B2BUA) functionality			
xii. Resource and admission control			
xiii. Network Address Translation (NAT) and Network Address and Port Translation (NAPT) Traversal			
xiv. Call Detail Record generation			
xv. Performance measurement (e.g., delay, jitter, and packet loss)			
xvi. Facilitating the forwarding of an emergency call/session to an Emergency Service Routing Proxy (ESRP)			
b. Border Firewall functionality including:			
i. Application and network layer protection and scanning			
ii. Denial of Service (DoS) detection and protection			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
iii. Scanning and elimination of known malware attacks			
iv. Access control through the use of access control lists and port-based permission/denial management			
v. Intrusion Detection			
vi. Receipt and update of 9-1-1 Malicious Content filtering			
c. Media Anchoring			
d. Virtual Private Network (VPN) bridging/mediation support			
e. Call Suspicion/Bad Actor Functions			
2. Emergency Service Routing Proxy (ESRP), that supports the following functionality, as described in NENA-STA-010.3f-2021			
a. Geographically-based routing to next hop			
b. Default/alternate routing to destinations served by the same ESInet, served by other ESInets via fully functional i3 NNIs, and other destinations outside of the serving ESInet, with available callback information, location information, and additional data provided, as appropriate			
c. Policy-based routing via interactions with a Policy Routing Function (PRF)			
d. LoST interface to an Emergency Call Routing Function (ECRF)			
e. Location and Additional Data dereferencing, using credentials traceable to the PSAP Credentialing Agency (PCA)			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
f. HyperText Transfer Protocol Secure (HTTPS) interface to Additional Data Repository for Additional Data dereferencing			
g. A web service interface to an Identity Searchable Additional Data Repository (IS ADR) to retrieve data stored by an entity that is not in the path of the call or access network			
h. HTTP-Enabled Location Delivery (HELD) and SIP interfaces to Location Information Servers (LISs) for location dereferencing			
i. Delivery of location and Additional Data by value and by reference			
j. Call delivery to i3 PSAPs and to legacy PSAPs (via appropriate gateways)			
k. Processing of “OPTIONS” transactions used as a “keep alive” mechanism			
l. Support for the client side of the ElementState and ServiceState event notification packages and the server side of the ElementState event notification package			
m. Supports an interface to a logging service to log every transaction and every message received and sent on its call interfaces, every query to the ECRF, every dereference request generated, and every state change it receives or sends			
n. Signature-based Handling of Asserted information using toKENs (SHAKEN) verification of signed caller identity information, and conveyance of the signed caller identity information, attestation level, and verification status information to the next hop/PSAP			
3. Policy Routing Function (PRF) that evaluates one or more policy rule sets (that conform to standard syntax and			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
semantics) to support the ESRP in determining the next hop for a call, as described in NENA-STA-010.3f-2021. Describe the mechanism used by the PSAP to manage the rules used by the PRF.			
4. Emergency Call Routing Function (ECRF) that supports the following functionality, as described in NENA-STA-010.3f-2021			
a. Operates as a standards-compliant Location-to-Service Translation (LoST) server that supports Geographic Information System (GIS)-based call routing in response to queries from authenticated entities			
b. Supports provisioning of GIS data via the Spatial Interface (SI)			
c. Supports the server-side of the Element State and Service State notification mechanism			
d. Supports the Service/Agency Locator function by receiving LoST queries to find a given service or agency by type and location			
e. Supports identification of transfer-to PSAP			
5. Location Validation Function (LVF) that supports the following functionality, as described in NENA-STA-010.3f-2021			
a. Standards-compliant LoST server that supports validation of civic location information to ensure that 9-1-1 calls will route and plot properly			
b. Supports periodic re-validation of stored location			
c. Supports provisioning of GIS data via Spatial Interface (SI)			
d. Supports the server-side of the Element State and Service State notification mechanism			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
6. Legacy Network Gateway (LNG) that supports the following functionality, as described in NENA-STA-010.3f-2021			
a. Interconnection to wireline end offices or Mobile Switching Centers via Multi-Frequency (MF) or Signaling System No. 7 (SS7)-supported trunks			
b. Standard interworking that converts MF signaling or SS7 protocol to the SIP protocol			
c. Interworking of Time Division Multiplexing (TDM) voice to Real-time Transport Protocol (RTP) data			
d. Interworking between Baudot tones and RFC 4103 real-time text			
e. Support for early media			
f. NG9-1-1-specific interworking functionality including:			
i. Identification of target ESRP address by interacting with an ECRF via a LoST interface			
ii. Generating a data structure that contains Additional Data about the call, along with a pointer/reference to that data structure (if conveyed by reference)			
iii. Handling of received Additional Data dereference requests			
iv. Delivery of calls to the ESRP with callback information and location (“by value” in the form of geo-coordinates or civic location, or “by reference”) using SIP signaling			
v. Support for transfers involving 9-1-1 callers connected to Legacy Network Gateways			
vi. Support for turn-taking associated with TTY interworking			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
g. Location interworking functionality including:			
i. Retrieving location information from a location database/server (e.g., Location Database [LDB]) based on calling number/Automatic Number Identification (ANI), Emergency Services Routing Key (ESRK), Emergency Services Routing Digit (ESRD), Emergency Services Query Key (ESQK)			
ii. Generation of a location reference, as appropriate for the call type			
iii. Handling of location dereference requests and associated signaling interworking (e.g., between HELD and E2)			
iv. Interactions with the MSAG[7] Conversion Service (MCS) if the location information retrieved from the location database/server is in civic format			
h. Support for Element State and associated event notification package			
7. Legacy PSAP Gateway (LPG) that supports the following functionality, as described in NENA-STA-010.3f-2021			
a. Interworking that converts SIP protocol to traditional MF or Enhanced MF, as appropriate for the interconnected PSAP, to support call delivery			
b. Accepting Dual Tone Multi-Frequency (DTMF) signaling (e.g., associated with transfer requests) from the legacy PSAP and converting it to RTP packets			
c. Interworking between RFC 4103 real-time text and TTY			
d. Interworking of Message Session Relay Protocol (MSRP) text and TTY			
e. NG9-1-1-specific interworking functionality including:			

[7] Master Street Address Guide

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
i. Mapping from non-North American Numbering Plan (NANP) callback information to a locally significant digit string (i.e., a pseudo-callback number formatted as a pseudo-ANI [pANI])			
ii. Association of a pANI with location information received via SIP signaling			
iii. Handling of transfer requests initiated by legacy PSAPs, including the creation of Emergency Incident Data Objects (EIDOs)			
iv. Conversion from MSRP text to RFC 4103 text			
v. Support for turn-taking associated with TTY interworking			
vi. Terminating and responding to test calls			
vii. Handling of Advanced Automatic Crash Notification calls			
f. Location interworking functionality including:			
i. Support for standard ALI query/response interface protocols			
ii. Initiation of location dereference requests			
iii. Initiation of Additional Data dereference requests			
iv. Interworking of relevant NG9-1-1 data elements to a standardized ALI format for population in ALI response messages			
v. Interactions with the MSAG Conversion Service (MCS) if the location information received in incoming signaling (or obtained via dereferencing) is in civic format			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
g. Support for the server side of the Element State event notification package			
8. Legacy Selective Router Gateway that supports the following functionality, as described in NENA-STA-034.1-2022			
a. Interconnection to legacy Selective Routers via SS7-supported trunk groups			
b. Interworking that converts between SIP protocol and SS7 protocol (i.e., SIP-to-SS7 and SS7-to-SIP)			
c. Interworking of real-time text and TTY (real-time text-to-TTY and TTY-to-real-time text)			
d. Interworking of MSRP text and TTY			
e. NG9-1-1-specific interworking functionality including:			
i. Identification of target ESRP address by interacting with an ECRF via a LoST interface (ingress LSRG)			
ii. Generating a data structure that contains Additional Data about the call, along with a pointer/reference to that data structure (if conveyed by reference) (ingress LSRG)			
iii. Handling of received Additional Data dereference requests (ingress LSRG)			
iv. Handling of transfer requests initiated by legacy PSAPs that are served by Selective Routers, including the creation of EIDOs (ingress LSRG)			
v. Forwarding initial or transferred calls to an ESRP (ingress LSRG)			
vi. Handling of transfer requests received from a conference bridge or ESRP (egress LSRG)			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
vii. Selecting the outgoing route to the Selective Router based on the destination PSAP number/address provided in SIP signaling from the ESRP (egress LSRG)			
viii. Facilitating the "turn-taking" expected by TTY users involved in emergency calls (ingress LSRG and egress LSRG)			
ix. Mapping from non-NANP callback information to a locally significant digit string (i.e., a pseudo-callback number formatted as a pANI) (egress LSRG)			
x. Association of an Emergency Service Number (ESN)-appropriate pANI with location information received via SIP signaling (egress LSRG)			
xi. Handling of Advanced Automatic Crash Notification (AACN) calls (egress LSRG)			
f. Location interworking functionality including:			
i. Retrieving caller location information by interacting with legacy ALI systems using standard ALI query/response protocols (ingress LSRG)			
ii. Retrieving routing location by accessing provisioned data that maps the location key (i.e., ESRD/ESRK/ESQK) to a routing location that is chosen so that it will route the 9-1-1 call to the primary PSAP that is to receive the call (ingress LSRG)			
iii. Generation of location references, as appropriate for the call type (ingress LSRG)			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
iv. Handling of location dereference requests and associated signaling interworking (ingress LSRG)			
v. Support for standard ALI query/response interface protocols (ingress LSRG)			
vi. Support for standard E2 interface, as specified in NENA-STA-018.2-2021 (egress LSRG)			
vii. Initiation of location dereference requests (egress LSRG)			
viii. Initiation of Additional Data dereference requests (egress LSRG)			
ix. Identification of ESN associated with the 9-1-1 call (egress LSRG)			
x. Interworking of relevant NG9-1-1 data elements to a standardized E2 format for population in response messages to ALI systems (egress LSRG)			
xi. Interactions with the MSAG Conversion Service (MCS) if the location information received in incoming signaling (or obtained via dereferencing) is in civic format			
9. A Spatial Interface (SI) that provides a standard interface between an authoritative copy of GIS data and functional elements within an ESInet such as an ECRF and LVF, as described in NENA-STA-010.3f-2021			
10. The Location Database (LDB), described in NENA-INF-008.1, performs the function of the location database/server associated with a Legacy Network Gateway, as described in NENA-STA-010.3f-2021.			
a. The LDB can functionally serve as a legacy ALI and can be queried by the LNG using legacy ALI protocols or, consistent with NENA-STA-010.3f-2021, can reside within the LNG (with the interface to the LDB left to			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
implementation, but possibly consisting of a legacy ALI protocol, ALI Query Service [AQS], HELD or a proprietary protocol)			
b. The LDB handles queries that include the location key(s) (e.g., calling number/ANI, ESRK, ESRD, ESQK) received by the LNG in call setup signaling			
c. Like a legacy ALI, the LDB responds with location and additional data provisioned in it			
d. For wireless calls, the LDB must be capable of querying a Mobile Positioning Center (MPC)/Gateway Mobile Location Center (GMLC) to obtain location information			
e. The LDB may continue to be provisioned using existing service order-based processes/interfaces i. The shell records required to interact with MPCs/GMLCs for wireless calls and Voice over IP Positioning Centers (VPCs) for VoIP calls must exist in the LDB			
11. Time Server/Network Time Protocol that provides time accuracy within 1 ms of true time and supports sufficient backup so that it can provide local time if the ESInet is isolated from its time source, as specified in NENA-STA-010.3f-2021.			
12. MSAG Conversion Service (MCS) that provides conversion between PIDF-LO and MSAG data as described in NENA-STA-010.3f-2021, including the following functionality:			
a. Mapping from a PIDF-LO to an MSAG address formatted as an XML object conforming to NENA 02-010 Version 4			
b. Mapping from an MSAG address formatted as an XML object conforming to NENA 02-010 Version 4 to a PIDF-LO			
c. Provisioning via the SI			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
d. Supports a complete set of fields for each MSAG record, as defined by NENA-STA-015.10-2018, and a link between the MSAG record and street/address point records in the ECRF/LVF			
e. Supports the server side of the ElementState event notification package and the server side of the ServiceState notification event package			
13. GeoCode Service (GCS) that provides geocoding and reverse-geocoding as described in NENA-STA-010.3f-2021, including the following functionality:			
a. Takes a PIDF-LO that contains a civic address, and returns a PIDF-LO containing a geodetic representation for the same location (Geocode)			
b. Takes a PIDF-LO that contains a geodetic representation, and returns a PIDF-LO that contains a civic address for the same location (Reverse-Geocode)			
c. Supports provisioning via the SI			
d. Supports the server side of the ElementState event notification package and the server side of the ServiceState notification event package			
14. The Logging Service is used by all elements in an ESInet to log all significant events associated with the processing of a 9-1-1 call, as described in NENA-STA-010.3f-2021. The functionality provided by the Logging Service includes the following:			
a. A web service that supports the logging and retrieval of events			
b. Supports a Sesson Recording interface (SIPREC - RFC 7866) for recording media and associated metadata			
c. Supports a Real-time Streaming Protocol (RTSP) interface compliant with RTSP 2.0 (RFC 7826) to play back media			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
d. Supports the server side of the ElementState event notification package and the server side of the ServiceState notification event package			
e. Handles signed and unsigned LogEvents and certain signing algorithms based on policy; if signed LogEvents are supported, the Logging Service must be capable of verifying the signature of a signed LogEvent during the processing of the LogEvent request			
15. Service/Agency Locator which, as described in NENA-STA-010.3f-2021, is a distributed database that provides a directory of agencies/services along with key information about the service or agency. The Service/Agency Locator supports the following two components: • A Service/Agency Locator Record Store (SALRS) that holds the actual data record for the service or agency, along with support for HTTPS GET to retrieve a record from the record store • A search component that uses the ECRF and a LoST query to find a given service or agency by type and location; searches by name should also be supported			
a. Data returned in response to a Service/Agency Locator dereference request is in the form of a JSON data structure containing the elements specified in Section 4.15.4 of NENA-STA-010.3f-2021.			
b. Each functional element in the Service/Agency Locator must implement the server-side of the ElementState event notification package.			
c. The set of Service/Agency Locator FEs within an ESInet must implement the server-side of the ServiceState event notification package for the Service/Agency Locator.			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
16. Bridging functionality is used in NG9-1-1 to transfer calls and conduct conferences, as described in NENA-STA-010.3f-2021. The functionality provided by a bridge in an NG9-1-1 environment includes the following:			
a. Supports a SIP signaling interface to create and maintain conferences			
b. Supports multimedia (voice, video, text)			
c. Provides media mixing			
d. Depending on the implementation, the bridge may be involved in the establishment of the initial emergency call or may only be invoked when needed during transfer or when conferencing more than two parties. Please indicate whether your NGCS solution supports one (and if so, which one) or both models.			
e. Supports Attended Transfers			
f. When an emergency call is transferred, the bridge inserts a reference to an Emergency Incident Data Object (EIDO) structure that contains location information and Additional Data obtained by the transfer-from PSAP during the processing of the 9-1-1 call			
g. When an emergency call is transferred, the bridge identifies itself as the originator of the call leg, the transfer-from PSAP as the originator of the transfer, and the transfer-to PSAP to which the call is to be directed.			
h. An emergency call that is transferred to a PSAP that is served by an interconnected ESInet/NGCS shall use a fully functional i3 NNI between the bridge in the ESInet that serves the transfer-from PSAP and the interconnected ESInet/NGCS			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
i. Supports bridging for MSRP text, where the text media streams are not mixed (i.e., are kept independent)			
17. The Outbound Call Interface Function (OCIF) is responsible for handling calls originating from i3 PSAPs over their serving ESInet/NGCS, including callback calls, official calls from one Public Safety agency to another (on the same or different ESInet), and administrative calls that have been promoted to emergency calls, as described in NENA-STA-010.3f-2021. The functionality provided by the OCIF includes the following:			
a. The OCIF will operate as a SIP proxy server, and may operate as a B2BUA in some circumstances, routing callback calls and, where appropriate, support calls to interconnecting networks			
b. The OCIF supports SIP/RTP interfaces that conform to Section 4.20 of NENA-STA-010.3f-2021			
c. The OCIF must be capable of handling outbound calls destined to the PSTN and may support interworking of SIP to SS7 through a standard PSTN Gateway. (Alternatively, PSTN access may be provided by an interconnecting network performs the signaling interworking.)			
d. The OCIF must support all media types identified in NENA-STA-010.3f-2021			
e. The OCIF interacts with a Secure Telephone Identity Authentication Service (STI AS) functional element to assert the telephone identity of the caller (i.e., PSAP) originating the callback or other PSAP-originated call			
18. Access to a Forest Guide by ECRFs and LVFs, as described in NENA-STA-010.3f-2021. A Forest Guide may be used to refer requests between ECRFs that possess different levels of ECRF data.			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
a. The Forest Guide will be queried by ECRFs/LVFs via a LoST interface			
b. A LoST-sync interface will be used for updating the coverage regions of the Forest Guide			
c. The Forest Guide must implement the server-side of the ElementState event notification package			
19. The Secure Telephone Identity Verification Service (STI-VS) functional element provides verification services applicable to emergency calls that are presented to the ESInet/NGCS with Signature-based Handling of Asserted information using toKENs (SHAKEN)-compliant signaling to provide caller identity verification services, as described in NENA-STA-010.3f-2021.			
a. The STI-VS must be capable of receiving SIP signaling (INVITE messages) from ESRPs			
b. The STI-VS must verify the signatures used to sign the caller identity information provided with the emergency call using the mechanisms defined in ATIS-1000074 and IETF RFC 8224, with the clarifications provided in Section 4.21.1 of NENA-STA-010.3f-2021			
c. The STI-VS must populate the appropriate “verstat” value in the signaling returned to the ESRP or return the appropriate error indication, as specified in Section 5.3.2 of ATIS-1000074.			
20. The Secure Telephone Identity Authentication Service (STI-AS) is a functional element that provides caller identity assertion for callback calls and other internetwork PSAP-originated calls. The STI-AS FE asserts and cryptographically signs the telephone identity of the caller, as described in NENA-STA-010.3f-2021.			

Respondent shall provide an NGCS solution that includes (at a minimum) the following functional elements and interfaces. Each element must meet or exceed the identified NENA standard.	Complies	Does Not Comply	Partially Complies
a. The STI-AS must be capable of receiving SIP signaling (INVITE messages) from an OCIF			
b. The STI-AS must honor the attestation level provided by the OCIF and then perform the STI-AS functions as described in ATIS-1000074 and IETF RFC 8224 i. The STI-AS requests its private key from the Secure Key Store (SKS) then use its private key to sign the caller identity ii. The STI-AS generates a cryptographically signed Personal Assertion Token (PASSporT) and inserts the PASSporT in an Identity header field that is included in the SIP INVITE message returned to the OCIF			

Details to support the response:

Originating Service Provider and Selective Router Migrations

Respondent shall provide the following services to support OSP interconnection with the ESInet and NGCS:	Complies	Does Not Comply	Partially Complies
1. Certificate to operate as a CLEC[8] in ETCOG's service area			
2. OSP connectivity in support of wireline, wireless, and VoIP traffic, as well as multiline telephone systems (MLTS)			
3. Coordinate with ETCOG to obtain a letter of authority/agency			
4. Establish interconnection and commercial agreements, and trunking in alignment with industry standards (e.g., ATIS-0700015), best practices, and regulations			
5. Provide an interface control document (ICD) for all OSP, CHE, and other 3rd party providers requiring ESInet connectivity			

[8] Competitive Local Exchange Carrier.

Respondent shall provide the following services to support OSP interconnection with the ESInet and NGCS:	Complies	Does Not Comply	Partially Complies
6. Coordinate with all telecommunications providers and manage circuit order processes to include testing and integration			
7. Describe the process for analyzing current trunk engineering for 9-1-1 traffic, and validating any trunk rebalancing for public safety-grade service			
8. Manage all adds, moves, changes, and deletions of connections to OSPs, both TDM[9] and IP-based, monitor these connections, and proactively work with the respective OSPs to resolve problems as they occur			
9. Coordinate and execute connectivity to legacy selective routers to support receipt of initial 9-1-1 calls, 9-1-1 call delivery to PSAPs served by legacy selective routers, and transfers to neighboring agencies not served by ETCOG's NG9-1-1 solution, including considerations related to bridging functionality and conveyance of call/incident information			
10. Define and manage all processes associated with split rate centers, local number portability, national number portability			
11. Support both TDM (via Legacy Selective Router Gateways and Legacy Network Gateways) and SIP ingress to the ESInet			
12. Provide a formal OSP Migration Plan that addresses: a. The OSP migration methodology, including a communications strategy b. Identification of POIs and type of ingress connectivity to be established c. Methodology and timelines for procurement, installation, support and maintenance of all hardware, software and networking required to support ingress connectivity d. Testing and turn up of connectivity to POIs			

[9] Time-Division Multiplexing.

Respondent shall provide the following services to support OSP interconnection with the ESInet and NGCS:	Complies	Does Not Comply	Partially Complies
e. OSP migration schedule f. Mechanism for reporting the status of OSP migrations to ETCOG g. Roles and responsibilities for the Respondent, ETCOG, and the OSP with respect to OSP migrations			

Details to support the response:

ALI Transition

Respondent shall provide the following services to support the transition from legacy ALI[10] to i3 functional elements:	Complies	Does Not Comply	Partially Complies
1. Service order input process for subscriber records			
2. Integration and provisioning for MLTS databases			
3. pANI[11] provisioning and shell records management			
4. Provisioning and management of pANIs utilized by Legacy PSAP Gateways and egress Legacy Selective Router Gateways, as described in Section 6.2.2.1 of NENA-STA-010.3f and Section 3.2.2.1 of NENA-STA-034.1, respectively			
5. Manage the transition to include coordination of all provider records from the legacy ALI database to the replacement LDB and any dual provisioning necessary during the transitional phases of the project			
6. Provide reporting for all data within the LDB via a web-based tool			

Details to support the response:

Text-to-9-1-1

[10] Automatic Location Identification.
[11] Pseudo Automatic Number Identification.

Respondent shall provide an NGCS solution that supports text-to-9-1-1 capabilities:	Complies	Does Not Comply	Partially Complies
1. Support for text delivery using Message Session Relay Protocol (MSRP)			
2. Support for Real Time Text (RTT) capability			
3. Support for transcoding between Baudot tones and RTT (i.e., RFC 4103-based real-time text) and vice versa			
4. Delivery of text messages via the ESInet to PSAPs from current TCC providers operating within ETCOG's service area			
5. NGCS can provide policy-based routing on incoming text messages			
6. Supports text transfers from PSAP to PSAP across the ESInet and between PSAPs served by the ETCOG ESInet and PSAPs served by different ESInets			
7. Text transfers include, at a minimum, caller identity and location information. Where available, transferred texts should include conversation history.			

Details to support the response:

Text Control Center (TCC) Services

Respondent shall provide Text Control Center Functionality for ETCOG	Complies	Does Not Comply	Partially Complies
1. Respondent provides or contracts TCC capabilities currently			
2. Respondent will provide TCC functionality to jurisdictions without TCC services as part of their NGCS deployment			

3. Respondent or respondent's contracted TCC receives text messages and provides 9-1-1 routing for all major wireless OSPs today			
4. Support for interconnection to third-party TCCs			

Details to support the response:
Respondent shall provide a description of their TCC partnerships and NGCS routing integration for text.

Logging/Recording and Reporting

Respondent's solution must provide the following logging/recording and reporting capabilities:	Complies	Does Not Comply	Partially Complies
1. Support for logging and retrieval of all relevant i3 events (as defined in Section 4.12, "Logging Service" of NENA-STA-010.3f-2021) via web service interfaces to a minimum of two Logging Services			
2. Each Logging Service functional element must implement the server-side of the ElementState event notification package			
3. The set of Logging Service functional elements within an NGCS must implement the server-side of the ServiceState event notification package			
4. The Logging Service must operate as a Session Recording Server (SRS) and implement a Session Recording Protocol interface, as specified in RFC 7866, for recording of media and, if provided, the associated metadata			
5. All Bridge elements, gateway elements, BCF elements that anchor media, and PSAP Call Handling elements, must implement the Session Recording Client (SRC) side of the Session Recording Protocol interface, and must insert a Call Identifier and Incident Tracking Identifier (in Call-Info header fields) into the SIP signaling (INVITE) sent to the Logging			

Respondent's solution must provide the following logging/recording and reporting capabilities:	Complies	Does Not Comply	Partially Complies
Service; elements acting as an SRC may also send the associated metadata to the Logging Service			
6. Discrepancy reporting (in the form of a web service), is supported by all NGCS functional elements to allow the reporting of data errors/discrepancies, following the mechanism described in Section 3.7 of NENA-STA-010.3f-2021			
7. Support for Alarm notifications to the PSAP (e.g., through a third-party and/or via ASAP[12] [as specified in APCO/TMA ANS 2.101.3-2021], or via an ESInet/NGCS [i.e., as a non-interactive call, as specified in NENA-STA-010.3f-2021]); describe mechanism used			
8. On-demand dynamic reports from the reporting UI			
9. Multitenant partitioning of logs and call data, allowing for partitioned reporting, based on role, PSAP or agency			
10. System must support the following built-in reports: a. Call reports by day/week/month (number of total calls, wireless/wireline/VoIP calls, abandoned calls, geospatially routed calls, policy routed calls, transferred calls, etc.) b. SIP error reports (within the ESInet) c. ECRF and LIS/LDB location queries and results d. ESRP/PRF routing reports (errors and successes) e. Location discrepancy reports f. Call volume and time to answer reports g. Additional Data queries and results			
11. Support for ad hoc reports by custom date/timestamp range, and creation of customized report templates			
12. Support for automated report generation and distribution			

Details to support the response:

[12] Automated Secure Alarm Protocol.

Credentialing

Respondent must be able to acquire and manage credentials traceable to the PSAP Credentialing Agency (PCA):	Complies	Does Not Comply	Partially Complies
1. Respondent must be capable of acquiring certificates from an NG9-1-1 Interoperability Oversight Commission (NIOC) PCA-vetted Intermediate Certificate Authority (ICA) and validating NIOC PCA Certificates for authenticity			
2. Respondent's solution interoperates with the NIOC PCA for credentialing (vendor NIOC PCA implementation through its own ICA, or a state or regional NIOC ICA)			
3. Solution utilizes certificate-based role authentication in alignment with the PCA, as outlined in NENA-STA-010.3f 2021 and in accordance with the NG9-1-1 Interoperability Oversight Commission (NIOC) Certificate Policy			
4. Supports the authentication of roles using a certificate obtained from the NIOC PCA			
5. All elements within the ESInet have credentials traceable to the PCA which can be used with mutual authentication methods; mutual authentication must be used for TLS and SIP session establishment using a certificate traceable to the PCA			
6. Solution supports credentialing with a Forest Guide and hierarchical ECRFs when integrated with state or adjacent NG9-1-1 solutions			

Details to support the response:

NGCS Availability and Reliability

Respondent's solution must comply with the following Availability and Reliability requirements:	Complies	Does Not Comply	Partially Complies
1. Solution must provide geo-diverse, and locally redundant NGCS			
2. All mission critical systems shall provide at least two geographically redundant systems that are each capable of processing 100 percent of the potential system load			
3. Solution must be locally redundant at hardware and software application layers			
4. Solution must maintain 99.999 percent availability			
5. Failure of any single instance of a hardware or software element or physical connection shall not negatively impact overall solution performance			
6. All network-connected elements must support at least two redundant and geographically diverse network interfaces			
7. All powered systems must include a minimum of two redundant power supplies (each of which must be able to power the system alone, and which would be connected to separate circuits) OR be connected to a power-transfer device that allows a single power supply to be connected to two isolated power sources (i.e., circuits) with automatic, uninterrupted failover, if the primary circuit fails.			
8. As supply chain impacts were experienced during the global pandemic, ETCOG seeks confirmation that any committed plan and/or schedule communicated within this response will be maintained regardless of future "supply chain impacts"			

Details to support the response:
Respondent shall provide details on how the stated availability will be achieved.

Training

Respondent's solution/service must provide training on the following items:	Complies	Does Not Comply	Partially Complies
1. Respondents should provide a Training Plan for their proposed solution that includes, but is not limited to, the following: a. A description of the training methodology; b. Training objectives, content, and schedule (identifying if in-person, live remote, video, etc.); c. Roles and responsibilities for the Respondent and ETCOG; d. Contact information for assistance and technical support for all training courses and material. e. Sample training materials			
2. Respondents should describe the logistics of their training program as it applies to the categories below, including, but not limited to, the following: a. Preferred scheduling/cadence b. Class size c. Location d. Recording of training sessions e. Personalization f. Multilingual availability			
3. SI users' interface tools			
4. Reporting and logging tools			
5. Incident reporting and ticketing tools			
6. Dashboards			
7. Change-management requests, processes, and tools			
8. PRF policy management			
9. GIS tools and procedures			
10. Subscriber Order Input (SOI) update procedures			
11. LVF procedures			

Details to support the response:

Other Interconnections

Respondent's solution/service shall support the following other interconnections:	Complies	Does Not Comply	Partially Complies
1. Interconnection with Additional Data Repositories (ADRs) and Identity Searchable ADRs (IS-ADRs)			
2. Access to commercial third-party Location Information Servers (LISs)			
3. Access to i3-compliant call-handling solutions			
4. Access to legacy PSAPs via gateway systems			
5. Integration of all OSP-provided location and media types as specified in NENA STA-010.3f-2021 for delivery to CHE			

Details to support the response:

Service Level Agreements

Respondent shall commit to the following service level agreements:	Complies	Does Not Comply	Partially Complies
1. 24 x 7 x 365 NOC/SOC			
2. Ability to submit incident and trouble tickets by phone, email, or direct User Interface to the ITSM system			
3. Documented escalation processes, procedures, and personnel			
4. Call-processing capacity capable of 100 percent of busy hour call traffic, expandable by 50%.			
5. Ability to grow call-processing capability by 50 percent over contract duration without service disruption			
6. Adherence to SLAs outlined in the *Performance Standards and Service Level Agreements* section of this RFP and acknowledgement of penalties associated with failure to meet same			

Respondent shall commit to the following service level agreements:	Complies	Does Not Comply	Partially Complies
7. Support for SLA reporting tools and procedures as detailed in *SLA Reporting* section of this RFP.			

Details to support the response:

Documentation

Respondent shall provide the following:	Complies	Does Not Comply	Partially Complies
1. Detailed network architecture design (transitional and end state) showing functional elements and interfaces (intranetwork and internetwork)			
2. As-built solution design documentation to include configured parameters and policy-routing flows (planned design and actual implemented design) prior to system final acceptance			
3. Network interface specifications for ESInets including: originating network to ESInet/NGCS interconnection; ESInet to PSAP interconnection; as well as ESInet-to-ESInet and ESInet-to-legacy Emergency Services Network interconnection			
4. Standards-based network interface control document for CHE			
5. User's guide for all user-accessible solution elements			
6. Detailed network design drawings reflecting the physical and virtual IP paths provided to each PSAP, including what is provided by sub-contracted last mile providers and/or resellers, prior to beginning system testing			
7. Operations manuals for all tools and UIs			
8. Training plan			
9. Project implementation plan			
10. Pre-cutover acceptance test plan (ATP) for core network			

Respondent shall provide the following:	Complies	Does Not Comply	Partially Complies
11. Pre-cutover ATP per PSAP			
12. Security Audit Checklist			
13. SI user documentation			
14. Project staffing plan			
15. NOC/SOC user guides including change-management processes			
16. Final Master Project Plan (MPP) shall be delivered to the ETCOG within 60 calendar days of contract execution			

Details to support the response:

Service Validation

Respondent shall support:	Complies	Does Not	Partially Complie
1. Independent third-party validation of the solution's feature functionality			
2. SIP messaging logs, call detail records, and/or call logs to verify compliance with contractual obligations provided to independent third-party for validation at ETCOG's direction.			
3. Documentation of completed results from NGCS Acceptance Test Plans (ATPs)			
4. Documentation of completed results from each PSAP's ATP			

Details to support the response:

Personnel/Staffing

Respondent shall:	Complies	Does Not Comply	Partially Complies
1. Provide a certified project manager to lead the implementation of the Respondent's solution			
2. Provide a post-implementation client manager			
3. Provide access to Tier 2 staff for issue and trouble resolution			
4. ETCOG may request a change in project manager in the event of poor performance or lack of responsiveness. Respondent shall execute change within 30 calendar days, if requested.			

Details to support the response:

GIS

Respondent's solution shall:	Complies	Does Not Comply	Partially Complies
1. Support collaboration with ETCOG to facilitate GIS data development and maintenance resulting in the highest quality GIS data without coverage overlaps or gaps that could impact the delivery of 9-1-1 services			
2. Leverage ETCOG's GIS data for geospatial routing of 9-1-1 calls, and for responses to CHE LoST queries for police/fire/ems response agencies.			
3. Provide secondary quality assurance (QA) and coalescing of GIS data to identify any structural issues with the data (attributes, formatting, missing layers, etc.) as well as any gaps and overlaps for all GIS data provided			
4. Return report of errors in tabular format (CSV, XLS) • NGUID of feature with error			

Respondent's solution shall:	Complies	Does Not Comply	Partially Complies
• List of check(s) failed			
5. Provide a web interface and/or automated method to provision data to the SI and retrieve post-QA data for use with mapping and/or the computer-aided dispatch (CAD) system			

Details to support the response:

Tools

Respondent shall provide:	Complies	Does Not Comply	Partially Complies
1. Web interface tool for accessing the LDB to extract reports, view TN, MSAG, and GIS data, perform corrections related to Discrepancy Reports (DRs), add status notes, and view transaction history as needed to support subscriber validation processes			
2. Web interface tool for viewing and submitting incident and change tickets			
3. Online dashboard showing network, device, and monitoring/alarm status			
4. Web interface tool for viewing policy-routing configurations			
5. Web interface tool to access call detail records (CDRs), searchable by date/timestamp, callback number, etc.			
6. Call trace application showing SIP messaging (INVITEs, REFERs, SIP errors, etc.) as well as HELD, LoST, and ADR queries and responses			

Details to support the response:

Change Management

Respondent's change-management process must include the following:	Complies	Does Not Comply	Partially Comply
1. Documented change-management process including scheduled and emergency changes			
2. A Method of Procedure (MOP) with backout plan for review by ETCOG a minimum of 72 hours prior to planned maintenance activities			
3. Defined mechanism for ETCOG to request changes and receive updates on progress			
4. Defined backup procedures			

Details to support the response:

Pre-Cutover Acceptance Criteria

Respondent shall support the following:	Complies	Does Not Comply	Partially Comply
1. Confirmation and documentation of equipment configuration			
2. Confirmation and documentation of control, monitoring, and alarm solutions			
3. Confirmation that, upon cutover, elements of the solution will support the latest software version available			
4. ATPs and documentation provided 15 business days prior to testing and allowing for third party review at ETCOG's discretion			
5. Include a pre-cutover ATP that contains testing processes for all functional elements in the proposed solution			
6. Show that the test plan can be tracked and measured			

Details to support the response:

Cutover Coordination

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
1. Must coordinate cutover activities with all service providers, ETCOG staff and PSAP personnel. ETCOG will have final approval of all cutover schedules.			
2. A detailed cutover plan, along with coordination, conference calls and supporting documentation, must be provided to all participating parties			
3. ETCOG is responsible for review and approval of the cutover plan			
4. Respondent shall provide trained and capable technical and functional solution support, and the project manager shall be available and onsite the day of cutover			
5. Respondent shall describe in its proposal how many of its staff will be available during cutover, and their areas of expertise			

Details to support the response:

PSAP Acceptance Testing

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
1. A lab for testing CHE compatibility to ensure its software is certified and that releases work seamlessly.			
2. PSAP acceptance testing, which is the execution of the approved pre-cutover acceptance testing to confirm that the Respondent's solution operates as expected and that the PSAP is ready for cutover to the LIVE NG9-1-1 system.			

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
3. PSAP acceptance testing will cover PSAP-specific requirements such as policy validation and transfer capabilities with all expected functionality fully operational, such as conveyance of location and call/incident data, and the ability to transfer text conversations.			
4. PSAP acceptance testing shall be completed no less than 1 week and no more than 30 days before PSAP is scheduled to cutover.			
5. Implementation of a change control freeze at the completion of each PSAP's acceptance testing, except in extreme cases, to prevent any system maintenance activities from breaking functionality or otherwise rendering the PSAP no longer ready to cutover.			

Details to support the response:

System Final Acceptance

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
1. System final acceptance cannot start until all ETCOG-designated PSAPs have successfully cutover to the LIVE NG9-1-1 system. The final acceptance period must be sufficient to demonstrate the solution's performance and reliability. The period shall be 30 consecutive calendar days.			
2. Contract deliverables must perform in compliance with all RFP and contract requirements throughout the acceptance period, subject to the fault categories described in the *System Final Acceptance Fault*			

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
Categories section of this RFP. If a failure to comply occurs, ETCOG will provide a written notification to the Respondent and:			
a. The Respondent shall remedy the non-compliance per the *Service Levels* and *Service Management Performance Standard* sections of the contract and provide written notification of the remedy to ETCOG			
b. The final acceptance period will restart upon ETCOG's written notification of acceptance of the remedy, or three business days, whichever is less			
c. This procedure continues until compliance over the final acceptance period is achieved, at which time the contract deliverables will be deemed fully accepted and the acceptance notice will be mutually executed. Note that ETCOG will provide a Notice of System Final Acceptance once the period successfully completes.			

Details to support the response:

System Final Acceptance Fault Categories

Respondent shall indicate its understanding and acceptance of the following:
The following fault categories are defined for use during the final acceptance process. (See the *Incident Security Levels* section of this RFP for further details.) All ETCOG-detected faults will be documented, and the documentation will also include a limited but reasonable time in which the fault is to be resolved by the Respondent

Respondent shall indicate its understanding and acceptance of the following:
1. Priority One Fault — A critical system fault that renders the solution even partially inoperable. These faults are unacceptable to ETCOG
2. Priority Two Fault — A major system fault that significantly reduces the solution's performance and ability to function. These faults are unacceptable to ETCOG and must be resolved before ETCOG will accept the solution.
3. Priority Three Fault — A minor system fault that marginally affects system performance and functionality. These minor faults are operational in nature and only are acceptable while in the final acceptance phase. These faults must be resolved before ETCOG will accept the solution.
4. Priority Four Fault — A combination of minor system faults and items that are on the punch list. These are items that have minimal or no effect on system performance and functionality. These faults must have a mutually agreed resolution timeframe before ETCOG will accept the solution.

☐ Understood

Details to support the response:

Migration Plan

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
1. Within 60 days of contract signing, the Respondent shall provide a detailed migration plan that shall include a full description of the methods and procedures that will be employed to ensure a non-service-affecting migration from the current environment to the new system.			
2. The Respondent shall provide a recommended transition considering the complexity of the regional environment			
3. The transition plan will recommend a suggested order for agency migration and provide projected time durations to			

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
complete the specific site based on position count and other information the Respondent has obtained regarding the region's configuration			
4. The migration plan shall include a fallback procedure to restore ETCOG to a pre-migration operational state in the event of a catastrophic failure.			

Details to support the response:

Software Release Management

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall describe the frequency of scheduled software releases and the decision-making processes involved in deciding what features and defect resolutions to include in a scheduled release			
2. Maintenance releases and feature releases shall be provided to ETCOG at no cost while a maintenance agreement is in place. The Respondent shall advise of all defects to software and advise of decision-making processes and software update schedules for resolution			
3. The Respondent shall provide ETCOG with access to the Respondent's defect tracking system to allow ETCOG to track the progress of defect resolutions. The Respondent shall provide a detailed description of the process and provide training to ETCOG staff prior to system final acceptance.			
4. The Respondent must include in its proposal the procedure to manage and track changes made to the system. This is especially important when changes affect the performance			

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
of a particular device, and it needs to be returned to its former configuration. The configuration-management procedure shall be available to maintenance personnel and ETCOG staff.			

Details to support the response:

Project Management

Respondent's solution shall include the following:	Complies	Does Not Comply	Partially Complies
1. A high-level project plan and timeline that shows the entire project calculated from the date of contract signature			
2. A task-oriented Gantt chart based on the project plan and delivered in Microsoft (MS) Project, or another mutually agreed upon Project Management platform.			
3. The steps that will be followed so that no service interruptions occur			
4. The project plan should include, at a minimum:			
a. Data gathering			
b. ETCOG onsite testing			
c. Core component installation and functionality and interface testing			
d. ALI format and interface testing			
e. Integration of aggregated GIS data into SI			
f. Comprehensive test and acceptance plan for all network connections verifying complete interoperability with deployed CHE			

Respondent's solution shall include the following:	Complies	Does Not Comply	Partially Complies
5. A more detailed project plan, timeline, and a Gantt chart delivered in MS Project, due to ETCOG within 30 days of contract signing			
6. Conduct a kickoff meeting at ETCOG within 30 days of contract signing.			

Details to support the response:

Progress Reports

Respondent shall support the following:	Complies	Does Not Comply	Partially Complies
1. Weekly project calls			
2. Weekly written progress reports, distributed within 24 hours of the project call, that capture the minutes and action items from the weekly project call			
3. Weekly progress report must contain details relating to the following tasks:			
a. PSAP data gathering			
b. Staging and lab testing			
c. Device and circuit installation progress at each site			
d. Connectivity information for CHE provider			
e. ALI/LDB transition			
f. GIS data readiness			
g. NGCS provisioning/implementation status			
h. Issue tracking			
i. Pre-cutover testing			
j. Cutover schedule plans			

Details to support the response:

Artificial Intelligence and Machine Learning

Respondent's shall describe the following:	Complies	Does Not Comply	Partially Complies
1. Artificial intelligence and machine learning (AI/ML) capabilities of the proposed system.			
2. Plans to introduce/enhance AI/ML capabilities of the proposed solution.			
3. Opportunities for applying AI/ML technologies and techniques for intelligent, dynamic, and automatic call overflow and rerouting.			
4. Ability to recognize Telephone Denial of Service (TDoS) bad-actors and quarantine the unwanted traffic from ETCOG's PSAPs' call queues.			

Details to support the response:

ETCOG Unique Requirements

Respondent's solution must provide	Complies	Does Not Comply	Partially Complies
1. Multitenant operation and support			
2. Make-busy functionality, (e.g. abandon switch)			
3. Near-simultaneous conference and transfer			
4. Conference with, transfer to, and alternate route to 7/10-digit numbers			
5. Transition of all legacy services shall be the responsibility of the Respondent. As such the Respondent shall ensure			

Respondent's solution must provide	Complies	Does Not Comply	Partially Complies
migration of all legacy connections and associated costs are completed within 120 days of the NGCS system "go live" date.			
6. The Respondent will issue service credits to offset any legacy costs not transitioned within 120 days of the NGCS "go live" date effectively ensuring there is no "double billing" for legacy and Next Generation 9-1-1 costs.			
7. Except for construction costs, billing to ETCOG will not commence until the service is turned up.			

Details to support the response:

PERFORMANCE STANDARDS AND SERVICE LEVEL AGREEMENTS

Performance Standards and Terms

Service Level Agreement - An agreement between ETCOG and the Respondent that specifies, using clear and measurable criteria, such as deadlines, quantities, quality standards, or other defined metrics, the services that the Respondent will furnish.

Help Desk Availability - Help desk should be available to answer calls from ETCOG (via an agreed-upon telephone number), create trouble tickets and dispatch technicians on a 24-hour basis.

Access to Technical Staff - The time-of-day technicians are available to assist ETCOG remotely and/or onsite.

Regular Business Hours (RBH) - Hours between 8:00 a.m. and 5:00 p.m. Central Time.

Response Time - The interval is defined as the time that elapses from when a trouble ticket is officially logged in the system to when a technician or support staff member with the necessary skills begins working to resolve the issue detailed in the ticket.

Repair Time - The interval between a trouble ticket being created and the technology issue being resolved, or having an acceptable workaround in place, and all functions restored to

normal.

System Performance Standards and Reporting - Respondents must identify the SLAs and metrics for the system components that will be utilized to formulate the system performance measurements for each performance standard.

System Availability - The ESInet, NGCS, and all fully redundant Call Handling Host and standalone deployments must be available 99.999 percent of the time in accordance with Table 5, row #7 which details system uptime requirements.

All ETCOG-determined Call Handling standalone single threaded PSAPs must be available 99.9% of the time in accordance with Table 5, row# 8.

Service Level and Service Management Performance Standard - Services referenced here are limited to those provided under the agreement. All times are averages over a rolling 12-month measurement period. However, there are provisions for declaring an SLA violation in cases where repeated instances occur over a short period of time.

All time intervals are calculated to the nearest minute. Performance requirements are applicable to managed and non-managed services.

Technician Availability - Technicians will be available remotely and/or onsite as required, on a 24 x 7 basis.

Web-Based Trouble Reporting and Tracking - It is required that trouble reporting, and escalation tracking are submitted via a secure web-based portal.

Incident Severity Levels

Severity Level 1 – Critical

An incident shall be categorized as “Severity Level 1” if the incident is characterized by the following attributes: the incident renders a critical network component, system, or service unavailable, resulting in significant impacts to 911 service functionality and/or operations, prohibiting the execution of productive work; and affects either a group or groups of people, or a single individual performing a critical function. Examples of “Severity Level 1” incidents include:

- Isolation of any single site or sites from the rest of the network, resulting in the inability for affected sites to communicate with the rest of the network
- Complete loss of functional elements within the NGCS (e.g., ECRF, ESRP, etc.)
- Decrease in throughput equal to or greater than 20 percent of capacities at any data center
- Cybersecurity attack detected by the Respondent to be in progress or highly likely/imminent

- Incidents affecting critical 9-1-1 service functionality (in alignment with FCC Part 4 rules) resulting in
  - The inability to deliver emergency calls to a PSAP (9-1-1 or 10-digit).
  - 9-1-1 calls delivered without audio (where audio is expected)
  - 9-1-1 calls delivered without location information
  - 9-1-1 calls delivered without callback information

Severity Level 2 – Major

An incident shall be categorized as "Severity Level 2" if the incident is characterized by the following attributes: the incident (a) does not render a critical network component, system, or service, unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work; and affects either a group or groups of people, or a single individual performing a critical business function. Examples of "Severity Level 2" incidents include:

- Decrease in throughput equal to or greater than 20 percent on any one circuit
- Loss of redundancy (connectivity, application, hardware device, etc.)
- Inability to access Additional Data (service type, service provider, etc.)
- Call misroutes (delivery of calls to the wrong PSAP, voice or text)
- Loss of critical functionality resulting in high operational impact or risk to the public (inability to transfer calls, perform policy routing, etc.)

Severity Level 3 – Minor

An incident shall be categorized as "Severity Level 3" if the incident is characterized by the following attributes: the incident causes a group or individual to experience an issue with accessing or using a system, service, software, equipment or network component, or a key feature thereof, and a reasonable workaround is not available, but the incident does not prohibit the execution of productive work.

Severity Level 4 – Maintenance/Non-Service-Impacting

An incident shall be categorized as "Severity Level 4" if the incident is characterized by the following attributes: the incident causes a group or individual to experience an incident with accessing or using a system, service, software, equipment or network component, or a key feature thereof, and a reasonable workaround is available, therefore does not prohibit the execution of productive work.

Response Time - A qualified resource must acknowledge requests for assistance by ETCOG via phone or secure web portal and commence investigation of trouble within the timeframes identified in the table below.

Table 2: Response Time

Trouble Category	Response Time
Severity Level 1	15 minutes
Severity Level 2	30 minutes
Severity Level 3	Next Business Day
Severity Level 4	Next Business Day

Repair Time - Issues documented via the ticketing process will be resolved in the timeframes identified in the table below. Resolution may be either the final repair that returns the system to its normal functioning condition, or an ETCOG-accepted workaround accompanied by a plan to achieve the final repair.

Table 3: Repair Time

Trouble Category	Repair Time
Severity Level 1	2 hours
Severity Level 2	4 hours
Severity Level 3	48 hours
Severity Level 4	5 business days

Escalation - Escalation of problems is critical to the quality of service provided. In cases where an interval identified in the table below has elapsed from the time the ticket was created, a request for assistance to the next higher level of technical support must be executed.

Table 4: Escalation Intervals

Trouble Category	Interval
Severity Level 1	30 minutes
Severity Level 2	1 hour
Severity Level 3	36 hours
Severity Level 4	96 hours

Once an escalation has occurred, the Respondent will provide ETCOG with a status update within one half of the escalation interval based upon the severity level, and then every 72 hours until a resolution path is agreed upon.

IP Network Measurements and Reporting

Network Performance

The selected Respondent must measure and report on the network performance against the service levels monthly. For any circuit downtime, outages, or interruptions, the selected Respondent must provide a written report describing the degradation of service or outage, including the root cause and the plan to prevent similar occurrences in the future. Trend data must be supplied with this report that shows current and previous monthly performances.

Outage Reporting

In the event of an unplanned outage, the selected vendor must provide to ETCOG a Reason For Outage (RFO) report. This report will include the timeline, the cause of the outage, actions taken to resolve the issue, and any actions/processes to prevent similar outages from occurring in the future. ETCOG requires a preliminary report within one business day of the event and a final report within 15 business days to be measured from the beginning of the service affecting issue.

Root Cause Analysis Reporting

A Root Cause Analysis (RCA) Report will be provided by the vendor to ETCOG for any unplanned outage or other service-affecting incident that results in an SLA being missed. An initial written explanation of the problem and the planned resolution will be provided by the vendor within 7 business days, with a final report provided within 30 business days, measured from the beginning of the service affecting issue. This report will include: a clearly articulated description of the problem, an analysis of data gathered to identify contributing factors that caused the problem, identification of the root cause of the problem, and corrective actions taken to address the root cause(s) and prevent recurrence.

Bandwidth Management

ETCOG must be able to observe overall bandwidth usage and specific usage between sites. The selected Respondent's solution must be able to create detailed SLA monitoring reports in real time. ETCOG must be able to view real-time or near real-time bandwidth performance and utilization reports. The solution should automatically determine the traffic type and provide various views into bandwidth usage. A secure web-based portal or browser-enabled viewer is preferred.

Voice Quality and Quality of Service

Voice quality must be maintained at traditional Public Switched Telephone Network (PSTN) levels and have priority over any other IP traffic. The solutions in place today use the G.711 codec, and the network must support voice quality that meets or exceeds ITU-T-P.830 and must be able to maintain a Mean Opinion Score (MOS) standard rating of 4.0 or higher.

Network Management and Monitoring

The Respondent must staff a Network Operation Center (NOC)/Security Operation Center (SOC) to respond to network issues and meet the service levels stated within this RFP, and to monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems to identify anomalous activity that could be indicative of a security incident or compromise.

Proactive Monitoring

It is the responsibility of the Respondent to provide active monitoring of its circuits for all network performance indicators described in the *Monitoring and Alarming* section of the RFP. The selected Respondent must proactively generate incident tickets and alert ETCOG (in accordance with incident severity level tables above) regarding response times.

Service Level Agreement

A service level agreement (SLA) is a contract between a service provider and the end user, which stipulates and commits the service provider to a required level of service.

SLA Reporting

Respondent shall provide a description of its reporting tool. A secure online SLA reporting tool is preferred. SLA reporting tools are expected to include both real-time and/or near real-time performance data captures in no greater than five-minute averages. The SLA reporting tool shall summarize network performance metrics by hour, day, week, month, quarter, and year. The mechanism must deliver automated SLA results to ETCOG on a monthly schedule. Quality of Service (QoS) reporting shall present traffic by type. Reports shall include, at a minimum, statistics for latency, jitter, packet loss, and bandwidth utilization, and shall be available on demand with near real-time data. A secure web-based portal is preferred. Other relevant data also may be reported.

Respondent shall specify how it will conduct and provide end-of-month and end-of-quarter reviews, accounting for any degradation of service to include service failures, as well as incidents and problems, and their resolution.

Incidents shall be tracked via tickets, and the ticket contents shall be made available to ETCOG.

The network provider should have automated systems to track all SLA deliverables and provide ETCOG with monthly reports detailing the provider's performance.

SLA Violations

A. An SLA violation shall have occurred whenever the Respondent fails to meet any single performance level.
B. An SLA violation shall have occurred whenever the average of any single performance metric—such as response time, uptime percentage, or resolution time—over the preceding two-month period fails to meet the service level. This constitutes an "early warning" of an

unacceptable trend. In the event of such an early warning, the service provider and client will jointly review the performance data and develop a corrective action plan to address the declining trend.

SLA Violation Damages

Damages shall apply whenever:

- Any single-performance-item SLA violation occurs in two consecutive months
- Any single-performance-item SLA violation occurs the month following an occurrence of an SLA violation per item B in the *SLA Violations* section of this RFP (the "early warning" violation).
- Any single SLA violation as described in the *Performance Standards and Service Level Agreements* section of this RFP occurs for more than four hours.

A chronic service outage will be deemed to have occurred if ETCOG experiences more than six outage occurrences, as identified in the *Incident Severity Levels* section of this RFP, in a rolling 12-month period, or if a service outage occurs for more than 24 hours and is not the fault or negligence of ETCOG.

SLA-Specific Network Service Requirements

- Network Availability >/= 99.999%
- Latency </=50 ms
- Packet Delivery >/=99%
- Jitter </= 5ms latency one-way, end-to-end
- Less than 1 percent packet loss
- Granular web based QoS controls not limited to percentage allocations
- Proactive circuit monitoring and 5-minute proactive notification for circuit outage
- Real-time customizable packet-filtering portal
- Packet analytics storage for all packets for 90 days
- Accept and honor QoS markings—i.e., Differentiated Service Code Points (DSCP)—as presented by ETCOG equipment, and pass markings through the network unmodified

Installation

Less than 90 business days or 18 calendar weeks for each circuit to be installed and ready for turn up (activation and testing of the circuit). Any installation exceeding 90 days will result in one day's credit per circuit not delivered (calculated based on the monthly recurring charge for each affected circuit), applied to the first month's bill. In the event of unforeseen developments, ETCOG and the Respondent will promptly communicate via designated project managers to develop a mutually agreeable solution and timeline adjustment, ensuring transparency and effective resolution throughout the implementation process.

Table 5 – Service Level Requirements, Metrics, and Remedies

#	Definition	Measurement Method	Objective	Rights and Remedies
1	Final Master Project Plan (MPP) shall be delivered to ETCOG (for ESInet/NGCS) within 60 calendar days of contract execution.	Calendar Days	Delivery of MPP within 60 days	Failure to meet the objective shall result in a $5,000 credit or adjustment for each calendar day that the report is not delivered after the objective.
2	Contractor shall achieve all milestone dates identified in the MPP.	Calendar Days	Completion of MPP milestones on or before the date agreed by ETCOG and Offeror.	Any failure to meet the objective shall result in a $5,000 credit or adjustment for each calendar day that the milestone is not delivered after the objective (for milestones with a majority of the underlying task ownership being that of the Contractor and/or its subcontractors).
3	SLA Remedy Delivery – Timely credit or adjustment of remedies due to ETCOG for missed SLR objectives.	Calendar Days	Contractor's credit or adjustment shall be issued no more than 60 calendar days after written notice from ETCOG of a service level failure.	Each occurrence of an SLR remedy (credit or adjustment) that is not issued within 60 calendar days shall result in a $5,000 credit or adjustment for each calendar day that the credit or adjustment is not issued.

4	Contractor shall provide a ticketing interface and monitoring dashboard 24 x 7 x 365.	The monthly availability percentage equals the Scheduled Uptime less Unavailable Time divided by Scheduled Uptime per month multiplied by 100. Scheduled Uptime is based on 24 hours x number of days in the month x 60 minutes. The monthly Availability percentage shall be based on the cumulative total of all outage durations for each calendar month.	99.9%	Failure to meet the SLR objective for one month shall result in a $2,500 credit or adjustment.
5	When a manual (i.e., via phone call to NOC) emergent request is made to reroute calls to an alternate PSAP, call rerouting will be effective within three minutes from the time the PSAP call is answered by the NOC for pre-provisioned routes. If the request is for standard maintenance, the reroute will be effective within	Time from NOC call received by human to time the routing change becomes effective.	3 minutes (emergency) 7 minutes (maintenance) 20 minutes (new route)	Failure to meet the SLR objective shall result in a $5,000 credit or adjustment.

	seven minutes for pre-provisioned routes, and if a new route is required, that will be completed within 20 minutes of request.			
6	Contractor shall report all outages that potentially impact the delivery of 9-1-1 traffic to every affected PSAP to ETCOG within 15 minutes of the occurrence.	Any outage that potentially impacts the delivery of 9-1-1 traffic, regardless of traffic type.	Notification of PSAPs and ETCOG within 15 minutes or less.	Any failure to meet the objective shall result in a $5,000 credit or adjustment For each additional minute that the Contractor fails to meet the SLR objective, an additional $1,000 credit or adjustment will be due.
7	Redundant ESInet connectivity shall be provided to each CHE core or host site connection (except as described in the following requirement).	The monthly availability percentage equals the Scheduled Uptime less Unavailable Time divided by Scheduled Uptime per month multiplied by 100. Scheduled Uptime is based on 24 hours x number of days in the month x 60 minutes. The ESInet connectivity availability requires two diverse IP	99.999% availability (less than 5.26 minutes per year or 26.3 seconds per month of unplanned downtime)	Failure to meet the SLR objective for one month shall result in a 25% credit or adjustment of the amount at risk for the ESInet for all affected PSAPs. Failure to meet the SLR objective for a second consecutive month shall result in a 50% credit or adjustment of the amount at risk for the ESInet for all affected PSAPs for

		network connections to each PSAP. For those PSAPs where diverse IP network connections are not available and when approved by ETCOG the Individual ESInet connectivity SLR applies. The monthly Availability percentage shall be based on the cumulative total of all outage durations for each calendar month.		that month. Failure to meet the SLR objective for each additional consecutive month shall result in a 100% credit or adjustment of the amount at risk for the ESInet for all affected PSAPs for all such consecutive months plus an additional $25,000.
8	Non-redundant ESInet connectivity shall be provided to each end point standalone CHE and will only apply when diverse NG9-1-1 trunks are not available and when approved by ETCOG	The monthly availability percentage equals the Scheduled Uptime less Unavailable Time divided by Scheduled Uptime per month multiplied by 100. Scheduled Uptime is based on 24 hours x number of days in the month x 60 minutes. The monthly Availability percentage shall be based on the cumulative total of all outage durations for each calendar month.	99.9% (8.77 hours per year 43.83 minutes per month)	Failure to meet the SLA objective for one month shall result in a 25% credit/or adjustment of the MRC for the population served by that end-point PSAP that month. The second consecutive month of failure to meet the SLA objective shall result in a 50% credit/or adjustment of the MRC for the population served by that end-point PSAP that month. The third

				consecutive month of failure to meet the SLA objective shall result in a 100% credit/or adjustment of the MRC for the population served by that end-point PSAP that month.
9	Contractor shall transition or migrate all ingress traffic from legacy selective routers (LSRs) to its NGCS in accordance with the timeline established by the FCC Report and Order in the Matter of Facilitating Implementation of Next Generation 9-1-1 Services (NG9-1-1)[13]. All traffic shall be migrated as soon as the respective OSP supports SIP-based interconnection.	Decommissioning of legacy selective routers and elimination of associated costs	Successful decommissioning of legacy selective routers.	Failure to meet the SLR objective shall result in a $5,000 credit or adjustment per OSP for each month that the OSP is not connected to the NGCS via SIP.
10	Contractor shall require SIP-capable OSPs to connect via SIP in accordance with the timeline established by the FCC Report and	Elimination of TDM aggregation sites.	100% ingress SIP call delivery	Failure to meet the SLA objective shall result in a $5,000.00 credit/or adjustment per OSP for each month that the

[13] FCC 24-178 Facilitating Implementation of Next Generation 911 Services (NG911) - https://www.fcc.gov/document/fcc-takes-action-expedite-transition-next-generation-911-0

	Order in the Matter of Facilitating Implementation of Next Generation 9-1-1 Services (NG9-1-1). All TDM traffic shall be transitioned as soon as the respective OSP supports SIP-based interconnection.			OSP is not delivering calls via SIP.
11	Failure to provide updates to solution to conform to NENA i3 standards within 18 months of ratification.	Identification by ETCOG or its designee of i3 functionality not supported.	100% conformance to NENA i3 standards within 18 months of ratification.	20% credit or adjustment of amount at risk for the ESInet, NGCS as applicable, until conformance issue is resolved to ETCOG's satisfaction.
12	NGCS must forward voice calls with little or no degradation of voice quality of the call from the ingress demarcation point to the egress demarcation point, as measured and monitored by an automated MOS measurement tool between various ingress and egress points.	Ingress demarcation point shall be defined as the Protocol Interworking Function (PIF) of the LNG (TDM call delivery without Selective Router) or LSRG (TDM call delivery with Selective Router) or the ingress SIP interface on the SBC (SIP call delivery). Egress demarcation point shall be the call-handling-facing port of the ESInet/NGCS edge	Maintain a MOS score of 4.0 or better across the ESInet and through the NGCS to the CHE demarcation point.	Failure to meet the SLR objective for one month shall result in a 25% credit or adjustment of the amount at risk for the ESInet for all affected PSAPs that month. A second consecutive month failure to meet the SLR objective shall result in a 50% credit or adjustment of the amount at risk for the ESInet for all affected PSAPs

		router at affected call-handling sites.		that month. Each additional consecutive month failure to meet the SLR objective shall result in a 100% credit or adjustment of the amount at risk for the ESInet for all affected PSAPs that month.
13	NGCS will deliver 9-1-1 traffic including caller identity, location information, and Additional Data to the appropriate NG9-1-1 CHE.	Single outage with a duration of **six** minutes or more.	Preventing NGCS outages of six minutes or more.	100% credit or adjustment of the amount at risk for NGCS for the affected PSAP(s).
14	NGCS will deliver 9-1-1 traffic including caller identity, location information, and Additional Data to the appropriate NG9-1-1 CHE.	Single outage of greater than **two** minutes and less than six minutes.	Preventing NGCS outages greater than two minutes, but less than six minutes.	50% credit or adjustment of the amount at risk for NGCS for the affected PSAP(s).
15	Contractor shall provide SLA reports required by this contract for each month of activity during the term of the contract by the 10th business day of the following month.	Business Days	Contractor shall deliver accurate and complete reports by the 10th business day of the month following the end of the applicable reporting month.	Failure to meet the objective shall result in a $5,000 credit or adjustment for each business day that the report is not delivered after the objective.

16	Contractor shall provide a cybersecurity vulnerability notification upon recognition of a cybersecurity threat or breach within three business days of issue identification.	Business Days	Within three business days of the recognition of a vulnerability or identified cybersecurity threat or breach, Contractor shall notify ETCOG of the event and measures taken to mitigate impact and avoid future risk.	Failure to meet the objective shall result in a $5,000 credit or adjustment for each business day that the report is not delivered after the objective.
17	Contractor shall provide an initial RFO report for Priority One and Two issues within one business day.	Business Days	Contractor shall deliver initial RFO to ETCOG within one business days of service affecting issue.	Each occurrence of a failure to meet the objective shall result in a $5,000 credit or adjustment for each business day that the report is not delivered after the objective.
18	Contractor shall provide a final RFO report within 15 business days from the beginning of the service affecting issue.	Business Days	Contractor shall deliver final RFO to ETCOG within 15 business days from the beginning of the service affecting issue.	Each occurrence of a failure to meet the objective shall result in a $5,000 credit or adjustment for each business day that the report is not delivered after the objective.

ETCOG PSAP INFORMATION

FCC ID	County	PSAP
6402	Anderson	**Anderson County Sheriff's Office**
6472	Camp	**Camp County Sheriff's Office**
6473	Van Zandt	**Canton Police Department**
6477	Panola	**Carthage Police Department**
6483	Cherokee	**Cherokee County Sheriff's Office**
8596	Gregg	**Christus EMS (Secondary PSAP)**
6608	Gregg	**Gladewater Police Department**
6619	Gregg	**Gregg County Sheriff's Office**
	Gregg	**Host A**
	Smith	**Host B**
6675	Cherokee	**Jacksonville Police Department**
6753	Marion	**Marion County Sheriff's Office**
6777	Wood	**Mineola Police Department**
6814	Anderson	**Palestine Police Department**
6818	Panola	**Panola County Sheriff's Office**
6842	Rains	**Rains County Sheriff's Office**
6961	Upshur	**Upshur County Sheriff's Office**
6966	Van Zandt	**Van Zandt County Sheriff's Office**
6996	Gregg	**White Oak Police Department**
7009	Wood	**Wood County Sheriff's Office**
6696	Gregg	**Kilgore Police Department**

REQUIRED

CURRENT REFERENCES

Please provide three (3) references from similar firms for whom your organization provided like services specific to this RFP, other than ETCOG, who can verify performance as a vendor/service is preferred. **NOTE**: Inaccurate, obsolete, or negative responses may result in rejection of quote submissions.

1. Name: _____ Phone: _____

   Address: _____St/Zip _____

   Contact Name_____ Email:_____

   Contract Name/Title:_____

   # of years contracted:_____

   Service Description:_____

   _____

2. Name: _____ Phone: _____

   Address: _____St/Zip _____

   Contact Name_____ Email:_____

   Contract Name/Title:_____

   # of years contracted:_____

   Service Description:_____

   _____

3. Name: _____ Phone: _____

   Address: _____St/Zip _____

   Contact Name_____ Email:_____

   Contract Name/Title:_____

   # of years contracted:_____

   Service Description:_____

   _____

REQUIRED SUBMISSION DOCUMENTATION

Bid proposals/submissions are to include the following:

1) References (p. 78); (return with submission)
2) Completed Technical Qualifications compliance tables and narrative information (pgs. 13-62); (return with submission)
3) Completed Security Audit Checklist (see NENA-REF-012.2-2025); (return with submission)
4) Appendix I & Conflict of Interest form - signed; (return attachment with submission)
5) Appendix II - signed; (return attachment with submission)
6) Signed 'Affirmation & Signature' (p. 86) ; (**must** return with submission);
7) Attachment A: Pricing Sheet; (the pricing matrix is provided in a separate Excel file titled "Attachment A – Pricing Matrix." Instructions for completing the pricing matrix are located under the Instruction tab in the Excel file. Pricing shall be submitted wholly and separate from the technical response to this RFP and returned as an attachment with the submission.)

Attention: It is understood failure to provide the above items with a submitted RFP proposal will diminish award consideration and ETCOG has the right to mark the proposal as non-compliant and treat it as a no-bid at their sole discretion.

Note: Only RFP Proposals submitted with all the required documentation/response on this page shall be considered for award in conjunction with the Evaluation Criterion, (p.82).

ETCOG reserves the right to award the contract to the proposer whose RFP submission is deemed most advantageous.

PLEASE CHOOSE ONLY ONE OPTION FOR SUBMISSION

Option 1 - HARD COPY RFP SUBMISSION

Hardcopy submissions must be clearly identified on the outermost return envelope or packaging and must be received by the bid submission date/time of **Wednesday, February 3, 2027 at 11:00 A.M. (CST)** regardless of if by mail, courier/delivery services, or hand delivered, at:

East Texas Council of Governments (ETCOG)
Attn: Christine Weems, Strategic Procurement Mgr.
3800 Stone Road, Kilgore, TX 75662

Write: Company Name, RFP#PS-911ESIN26R , Wednesday, February 3, 2027 , in bottom left-hand corner of the outermost Return Envelope/Package

NOTE: Emailed, telephone, & facsimile bid submissions are not allowed in response to this RFP.

1. Proposers are to submit one (1) hardcopy marked 'Original' along with (4) four additional copies

marked 'Copy' and submit one (1) electronic copy of RFP proposal to include all related documentation. Please do not use 3-ring binders.

2. Pages should be numbered and contain an organized, paginated table of contents corresponding to the section and pages of the proposal. At least an eleven (11pt) point font of Calibri, Ariel, or Times New Roman is acceptable and must be legible.

3. It is the Proposer's sole responsibility to prepare, submit, and deliver or arrange delivery of the RFP proposal(s) with all required exhibits and materials to the designated location on or before the published submittal deadline.

4. ETCOG will not bear liability for any costs incurred in the preparation and submission of submissions in response to this RFP.

5. RFP submission deadline *time* will be determined by the ETCOG lobby clock.

6. If submitting more than one property to be considered, each property submission should be placed in a separate envelope and clearly identified with the RFP number, submittal deadline/opening date and time, as referenced on previous page.

7. Courier or delivery services may not deliver directly to the specified location; therefore, it is strongly recommended**:**

   - Proposers allow sufficient time for delivery of a hard copy proposal prior to the published deadline date/time to the location specified.

   - Proposers understand that failure to submit a proposal by designated deadline, for whatever reason, may not be grounds for disputing the procurement solicitation process or any resulting contract award.

8. It is the Proposer's sole responsibility to ensure any addenda or additional materials pertinent to their proposal be included in or with their RFP submission. ETCOG will not be held liable for missing addenda or materials at the time of the RFP Opening and said addenda or additional materials will not be accepted past the RFP submission deadline date and time.

Option 2 - DIGITAL RFP SUBMISSION OPTION

Upload Requirements/Instructions

1. Proposers must **email** Christine Weems at christine.weems@etcog.org to **request an 'Access Link' by 11:00 A.M (CST) on Tuesday, February 2, 2027**, if not sooner, to receive digital upload purposes.

2. Access code requests by phone, voicemail, or past the noted deadline date/time above will not be accepted, **no exceptions**.

3. It is the Proposer's sole responsibility to upload their RFP proposal digitally with all required exhibits and materials by referenced **'RFP Submission Due' deadline date/time (p. 1),** if not sooner.

RFP RETRIEVAL

The RFP document, related appendix, RFP bid updates, and any additional RFP information or amendments throughout the bid process will be posted as warranted on the ETCOG website and may be retrieved by clicking on the '**9-1-1 ESInet 2026 RFP**' link at Procurements or request by emailing Christine Weems at: christine.weems@etcog.org Please note, it is the Proposer's sole responsibility to stay informed of any RFP changes/updates.

PROPOSER COMMUNICATION

There is to be no communication allowed, in any form, between ETCOG and their representatives, other than conducting daily business unrelated to this RFP , during the entirety of the RFP process. Failure to follow this directive will result in rejection of Proposer participation and/or submitted RFP proposal.

QUESTION/RESPONSES

Proposer Questions: Proposer questions concerning this RFP are due **Monday, November 30, 2026 at 5:00 P.M. CST** if not sooner, and must be emailed to Christine Weems, Facilitator at: christine.weems@etcog.org and no one else.

Staff Responses: Proposers **must** go online at Procurements and click on **' 9-1-1 ESInet 2026 RFP**' to retrieve responses to all questions asked, no earlier than **Friday, December 4, 2026, at 5:00 P.M. CST**

NOTE: Other than the above opportunity and unrelated daily business, there is to be no communication between Proposers and ETCOG staff or representatives during an active RFP process to ensure fair and open competition for all potential Proposers. To willingly do so may result in the disqualification of a Proposer for non-compliance of RFP restrictions.

RFP RETRIEVAL

The RFP document, RFP updates, and additional RFP information or amendments will be posted on the ETCOG website and may be retrieved by clicking on '**9-1-1 ESInet 2026 RFP**' at Procurements or request by emailing to Christine Weems at: christine.weems@etcog.org

VETHUB & NONDISCRIMATORY BEST PRACTICES

VetHUB is a program that focuses on certification of service-disabled veterans to facilitate their growth and development and increase VetHUB contract and subcontracts with the State of Texas. ETCOG shall ensure veteran-owned businesses are considered as sources for acquisitions whenever possible by:

- soliciting these businesses whenever they are potential sources;
- when economically feasible, dividing total desired services into smaller components to permit

maximum participation by these businesses;

- if the requirement permits, establishing delivery schedules that will encourage VetHub to participate; and
- using the services and assistance of the VetHub list on the Texas Comptroller website, as needed.
- Vendors are encouraged to make a good faith effort to consider VetHubs when subcontracting.
- utilizing the Texas Comptroller of Public Accounts website Texas Comptroller of Public Accounts ;
- utilizing Web sites or other directory listings maintained by local Chambers of Commerce.
- advertising subcontract work in local veteran and minority publications; and/or contacting the contracting state agency for assistance in locating available VetHubs.

Please refer to Texas Government Code, Chapter 2161 for HUB and VetHUB general provision.

All vendors and their contractors and subcontractors shall comply with all applicable nondiscrimination and equal opportunity provisions of federal and state law and all regulations implementing the laws.

RFP EVALUATION AND SELECTION OF SUBMITTAL

ETCOG intends to evaluate proposers based on the criteria set forth below. ETCOG may review written submissions, request clarifications, conduct interviews, request presentations, negotiate scope and fees, and select the Respondent determined to be the most qualified and in the best interest of ETCOG.

EVALUATION CRITERIA TABLE

CRITERIA TABLE	POINTS
History-Background/Experience	**10**
System Integration and Interoperability	**10**
Technical Requirements	**30**
Implementation and Project Management	**5**
Operations and Maintenance	**10**
Cost Proposal (Pricing Matrix)	**25**
Compliance and Regulatory Adherence	**10**
TOTAL	**100**

NOTE: The number of proposals selected for consideration will be at the sole discretion of ETCOG.
A composite grade of a minimum of 70 points or more is required to be eligible for award consideration. The ratings will be based on the qualifications provided in the proposal by the closing date/time of the RFP.

RFP PROPOSAL REVIEW TERMS

1. RFP proposal submissions will be reviewed by ETCOG staff to determine if proposal meets program needs and if requested information and required documentation as identified throughout the RFP document has been returned to qualify for award consideration.

2. An evaluation team made up of staff, outside evaluators, committee members, and/or other subject matter experts as deemed necessary to achieve the best possible results will evaluate and score the submitted RFPs.

3. ETCOG reserves the right to contact any source regarding, but not limited to, vendor reputation, product/service quality, work history, and/or past performance to evaluate/award the bid submission(s) that best meet ETCOG program needs, and clients served.

4. The evaluation team's preferred proposal will be presented to governing body(s) as a recommendation for award so the governing body(s) may make a final award decision.

5. RFP submission must have original signature of the person having the authority to bind the organization to a contract or it may be rejected for non-compliance.

ETCOG GENERAL SELECTION TERMS

1. ETCOG will select only one proposer to perform the services.

2. ETCOG reserves the right to ask questions, request additional information or clarifications, hold individual interviews at any given time throughout the evaluation and negotiation process to determine the proposal which best meets the procurement needs being sought to the best benefit of ETCOG and programs served.

3. ETCOG reserves the right to allow corrections of non-material errors or omissions at ETCOG's sole discretion.

4. Submission of a RFP proposal indicates Proposer's acceptance of the evaluation and award process and is in agreement the evaluation team may make subjective judgments in evaluating the proposals to determine best value to best benefit ETCOG and programs served.

5. ETCOG reserves the right to accept or reject any bid proposal received, as well as cancel the RFP in its entirety at any time during the bid process, without notice or explanation, which may result due to unforeseen irregularities, low response, or procurement needs not being met by submitted proposals.

6. ETCOG may modify or waive any provisions set forth in this RFP for any reason and all herein mentioned without notice to anyone if deemed in the best interest of ETCOG and programs served.

7. ETCOG reserves the right to negotiate the final terms of any potential contract or service agreement resulting from this RFP to include but not limited to the RFP document, Proposer(s) submitted

proposal, and the RFP exhibits and Appendices I & II, i.e., 'ETCOG General Terms & Conditions,' and the 'Essential Clauses and Certifications' pages requiring signatures, all acting as binding documents to said contract or service agreement.

8. ETCOG reserves the right, should contract negotiations fail, to enter negotiations with the next highest ranked Proposer with a proposal considered best to meet program needs, and may continue in like manner until successful negotiations have been reached. Furthermore, although ETCOG has the right to negotiate with the next highest ranked Proposer, it is not required to do so and may re-procure or cancel the RFP at ETCOG's sole discretion.

9. Proposer shall indemnify and hold harmless ETCOG, its officers, agents, and employees from any injuries or damages received by any person during any operations connected with the contract, by use of any improper material, or by any act or omission of the contractor or his subcontractor, agents, servants, or employees.

10. Execution of any resulting contract or service agreement is required prior to processing any payments to the successful Proposer.

11. Pursuant to protocol to advise of the right to appeal, a protest must be submitted to ETCOG's Executive Director within ten (10) calendar days of the time the basis of the protest became known and said protest(s) limited to: 1) violations of federal law or regulations; 2) violations of State or local law under the jurisdiction of State or local authorities; and 3) violations of ETCOG's protest procedures for failing to review a complaint or protest. The protest must be submitted in writing and must identify the protestor, the solicitation being protested and specifically identify the basis for the protest, providing all pertinent information regarding the solicitation, contract and/or actions of ETCOG.

RFP PROPOSER COMPLIANCE

Proposer shall comply with all federal, state, and local laws, statutes, ordinances, rules and regulations, and the orders and decrees of any court or administrative bodies or tribunals in any matter affecting the performance of the agreement including, if applicable, workers' compensation laws, minimum and maximum salary and wage statutes and regulations, and licensing laws and regulations. Proposers will be prepared to provide satisfactory proof of compliance if requested

RFP AWARD NOTIFICATION

It is expected an award will be presented at the **March 2027** ETCOG Executive Committee Meeting.
(date subject to change)

PUBLIC DISCLOSURE

No public disclosures or news releases pertaining to this Contract shall be made without prior written approval of ETCOG.

CONTRACT PAYMENT METHOD

Any resulting contracts are NET30 at the time the invoice is received by a.p@etcog.org in ETCOG Operations/Finance department. Payment will be made in accordance with the standard lease terms or agreement.

REQUIRED

SIGNATURE PAGE

Proposer affirms understanding and acknowledgement of all referenced bid and program requirement contained within the RFP document; Appendix I - ETCOG Terms and Conditions/Conflict of Interest Questionnaire (CIQ) form; Appendix II - Essential Clauses & Certifications; Attachments and any Exhibits (if provided) are explicit to this bidding procurement and Proposer must return any and all such pages requiring action, signatures, or checkmarks from the RFP document, Appendices, and Attachments with any submitted bid proposal. Proposer further understands and acknowledges making a false statement or proclamation of compliance is a material breach and any subsequent award of product/equipment purchase(s), offered services, and/or contract/service agreement is grounds for award cancellation.

SIGNATURE

The undersigned individual hereby certifies and warrants that he/she has been fully authorized to execute this proposal/bid submission on behalf of their firm and to legally bind the firm to all the terms, performances, and provisions as herein set forth.

Company/Provider Name	Phone Number
Signature	Date
Printed Name and Title of Authorized Representative	Email

IMPORTANT: Proposer must return this page fully executed and complete with proper signatures and signature dates for current/active RFP or the submitted proposal will be marked 'Rejected/No RFP' due to non-compliance.