CONTENTS

1 GENERAL REQUIREMENTS

1.1 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 differentiates its 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 call handling systems, comparable to the one being proposed for INCOG, that have been installed and are currently operational
g. References from 9-1-1 agencies (at least three that demonstrate similar implementation of the service model solution proposal). References should be in sealed envelopes from the reference and mailed to the address listed in Section [x.x].

☐ Understood

1.2 Interoperability

To ensure interoperability between the proposed i3 CHE solution(s) and all components of interconnected ESInet/NGCS solution(s), all Respondents must commit to, and document (prior to completion of contract negotiation), the interoperability of their CHE solution with available i3 ESInet/NGCS solutions. Respondent(s) must identify below all of the ESInet/NGCS solutions with which their solution(s) currently operates. Supporting documentation of interoperability is desirable and may take the form of references from customers where solutions have been deployed and operational for a minimum of six months.

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 the Indian Nations Council of Governments, Oklahoma 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.

2 INDUSTRY STANDARDS

The Indian Nations Council of Governments, Oklahoma (INCOG) seeks a standards-based solution that complies with nationally accepted standards and requirements applicable to IP network architecture,

[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

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:

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

Further, the Respondent's solutions and services shall comply with any additional standards, requirements, statutes, and policies as identified in specific sections throughout this document.

Table 1: Adopted Standards

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
APCO/TMA ANS (Formally known as CSAA)	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 ANS	1.102.3.2020	*Emergency Communications Center (ECC) Service Capability Criteria Rating Scale*	Provides an assessment tool to evaluate current capabilities of the ECC against models representing the best level of preparedness, survivability, and sustainability amidst a	Version 3, January 30, 2020

[2] *For any standards, if a newer version is available at the time of publication of this document, compliance will be judged relative to the latest version. The exception to this being NENA/APCO-INF-005.1-2014 for which compliance will be judged relative to NENA's updated Emergency Incident Data Object STA document*

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
			wide range of natural and manmade events.	
ATIS/TIA	ATIS J-STD-110.v002	*Joint ATIS/TIA Native SMS/MMS Text To 9-1-1 Requirements and Architecture Specification*	Defines the requirements, architecture, and procedures for text messaging to 9- 1-1 emergency services using native CMSP SMS or MMS capabilities for the existing generation and next generation (NG9-1-1) Public Safety Answering Points.	Release 2 May 1, 2015
ATIS	ATIS-0700015.v005	*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 5 June 2021
ATIS	ATIS-100074.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	Version 3 August 2022

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
U.S. Department of Justice	CJISD-ITS-DOC-08140-5.9	*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 5.9 June 1, 2020
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.	January 21, 2021
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	August 2008

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
			identifiers and geodetic or civic location information to service contact URIs	
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 geographic location information from one SIP entity to another SIP entity	December 2011
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 include IPv6 to include zone identifiers and address literals	July 29, 2020
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

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
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. Updates RFC 8373*	Specifies how a Web Real-Time Communication (WebRTC) data channel can be used as a transport mechanism for real-time text.	Version 1 January 2021
NENA	REQ-001.1.2-2018	*Next Generation 9-1-1 PSAP Requirements Document*	Provides requirements for functions and interfaces between an i3 PSAP and NGCS, and among functional elements associated with an i3 PSAP	June 10, 2018
NENA	NENA-STA-006.2a-2022	*Standard Data Formats for 9-1-1 GIS Data Model*	Defines the GIS data information, formats, requirements and related information used in NENA Next Generation 9-1-1 (NG9-1-1) Core Services (NGCS)	Revised September 23, 2022
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	October 6, 2014
NENA	NENA-STA-010.3e-2021	*NENA i3 Standard for Next Generation 9-1-1*	Builds upon prior NENA publications including i3	Version 3e

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
			requirements and architecture documents and provides additional detail on functional standards	January 30, 2024
NENA	NENA-STA-015.10-2018 (Originally 02-010)	*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 August 12, 2018
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	April 5, 2018
NENA	NENA-STA-027.3-2018 (Originally 04-001)	*NENA E9-1-1 PSAP Equipment Standards*	Defines the PSAP equipment requirements intended for use by users, manufacturers, and providers of E9-1-1 Customer Premises Equipment (CPE)	July 2, 2018
NENA	08-751	*i3 Technical Requirements Document*	Provides requirements for ESInet architecture and security, among other i3 PSAP functions, and establishes a foundation for future i3 standards development	Version 1 September 28, 2006
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	*Security for Next Generation 9-1-1 (NG-SEC)*	Establishes the minimal guidelines and requirements for levels of	November 4, 2024

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
			security applicable to NG9-1-1 entities	
NENA	75-502	*Next Generation 9-1-1 Security (NG-SEC) Audit Checklist*	Provides the educated user a method to document an NG-SEC Audit	Version 1 December 14, 2011
NENA	NENA-INF-008.1 (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	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.	July 27, 2022
NENA	NENA-STA-021.1a-2022	*NENA Standard for Emergency Incident Data Object (EIDO)*	Provides standard format for exchanging emergency incident data between disparate systems and agencies	Version 1a April 19, 2022
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

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[2]
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 Requirements for Cryptographic Modules*	Specifies security requirements that will be satisfied by a cryptographic module utilized with a security system protecting sensitive but unclassified information	Version 2 March 22, 2019
NIST	Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*	Provides standards, guidelines, and best practices that promote the protection of critical infrastructure	Version 1.1 April 16, 2018
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

2.1 Standards Evolution

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 and security industry standards within 18 months of ratification of applicable industry standards. 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 disclose any performance or feature changes prior to the upgrade and report them to the INCOG for approval.

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

3 TECHNICAL REQUIREMENTS – CALL-HANDLING SYSTEM

This Technical Requirements 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 supporting, or elaborating upon, the compliance declaration for the requirements in the table. While there are no limitations on the extent of this additional information, such information should be focused on the specific requirements being addressed. Concise details and brevity are encouraged. It is asked that, if no additional information is being provided for a particular table of requirements, that the Respondent include a statement to that effect (e.g., “N/A,” “None,” “No details provided,” etc.) to confirm that the lack of supporting information is deliberate and not an oversight.

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

3.1 CHE Network

Requirements:	Complies	Does Not Comply	Partially Complies
1. The implementation of new IP connectivity and the replacement, migration, or rehoming of any part of INCOG’s existing network, (including ESInet circuits, Vesta phone system, etc.), shall have the following requirements: a) Respondent shall work together with the ESInet provider to order, install, and test any new ESInet circuits, as well as collaborate over routing specifications (BGP, etc.) to accommodate the expected behaviors, (load sharing, circuit failover, etc.). b) Respondent shall work together with INCOG Regional Board representative to order, install, and test any new circuits, as well as collaborate over any expected behaviors therein.			

Requirements:	Complies	Does Not Comply	Partially Complies
c) Respondent's solution shall provide CHE network connectivity that supports INCOG's current call and data delivery functionality between agencies.			
2. Respondent shall provide redundant circuits into diverse entrance facilities at its datacenters.			
3. Respondent shall provide a minimum of one terrestrial (copper or optical circuit) connection with adequate bandwidth into each PSAP facility, (primary and backup).			
4. Respondent shall be capable of receiving and integrating 911 calls delivered over secondary wireless connections as implemented by INCOG and their ESInet / NGCS provider, (e.g. FirstNet other LTE network, Satellite, microwave, carrier-diverse fiber, etc.)			
5. The solution shall align with NENA STA-010.3e-2021, *Detailed Functional and Interface Specifications for the NENA i3 Solution,* (or its successor document, when ratified).			
6. The solution shall use open standards.			
7. The solution shall support and enforce quality of service (QoS) marking using Differentiated Service Code Point (DSCP).			
8. The solution shall provide network traffic convergence of less than 50 milliseconds (ms).			
9. The solution shall maintain a Mean Opinion Score (MOS) of 4.0.			
10. The solution shall scale to support call-volume growth by 50% without requiring replacement of any critical hardware or software component.			

Requirements:	Complies	Does Not Comply	Partially Complies
11. Failure of any single instance of a hardware or software element, or physical connection shall not impact overall solution performance.			
12. All network-connected elements shall support at least two redundant network interfaces with automatic failover between them.			
13. All powered devices supporting network connectivity for INCOG, (firewalls, routers, switches, etc.) shall include a minimum of two redundant power supplies (each shall be able to power the device alone) that 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.			
14. The Respondent shall describe how their solution supports the ability to log onto the proposed system from an off-site location should the Primary PSAP become inoperable.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

3.2 Call-Handling Solution Architecture

Requirements:	Complies	Does Not Comply	Partially Complies
1. INCOG requires the Respondent to provide a solution that is architected to support a Host-Remote deployment model with at least two geographically diverse host locations. “Host-Remote” in this instance refers to a “multi-tenant” architecture where multiple PSAPs will share the same call handling system that is comprised of at least 2 hosts. It can be hardware (traditional datacenter) centric or software (cloud) centric. If the respondent supports both a traditional datacenter-based solution and a cloud-based solution, please describe both and include separate pricing options in the response.			
a. If the Respondent supports a cloud-based solution, please provide a complete description of : • How the solution is managed • Redundancy in the solution • Whether the solution is cloud-hosted vs. cloud-native, • Whether the cloud used in the solution is DoD-compliant, CJIS-compliant **No part of the solution shall be hosted outside of North America**.			
2. Respondent’s CHE solution shall interoperate with the Oklahoma 9-1-1 Management Authority (OK911MA) statewide i3-conformant ESInet and NGCS. Until such time as the statewide ESInet/NGCS is available, the Respondent shall identify what IP network the CHE solution shall use in the interim.			
3. Respondent shall be responsible for working directly with the ESInet provider to troubleshoot any issues related to call presentation associated with the receipt or transfer of calls through OK911MA’s statewide ESInet. Respondent shall update INCOG and any designees on troubleshooting and progress weekly at a minimum.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

3.3 Security

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall describe how its security in-depth approach embodies the best practices outlined in the latest version of NENA-STA-040.2-2024, *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*.			
2. The Respondent shall include a security plan document that addresses, physical, application, and network security.			
3. The solution shall utilize end-to-end encryption for all sensitive data that transits CHE network (i.e., data in transit) preferably using Advanced Encryption Standard (AES) with a minimum key length of 256 bits (AES 256)			
4. The solution shall encrypt stored data (i.e., data at rest) that contains confidential information using AES 256 or an equivalently strong algorithm Please describe your “data at rest” policies such as AES, physical control, strong password requirements, monitoring, and configuration management.			
5. The solution shall support password security mechanisms such as requiring 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			

Requirements:	Complies	Does Not Comply	Partially Complies
example, the use of strong passwords and password expiry/change timeframes.			
6. The solution shall provide firewalls between call-handling nodes and their external connections.			
7. The Respondent shall ensure that all call-handling components interfacing with the OK911MA's ESInet / NGCS provider carry credentials traceable to the national PSAP Credentialing Agency (PCA).			
8. The Respondent shall describe how single sign-on (SSO) and multifactor authentication are supported in their call-handling solution to support user access management.			
9. The Respondent shall perform proactive analysis of the network for vulnerabilities including independent security audits of the solution.			
10. The Respondent shall have a defined continuity of operations (COOP) plan as well as a disaster recovery (DR) plan and shall include those plans with their response. The Respondent shall review their COOP and DR plans every 12-18 months and shall provide to INCOG either an updated copy or an explicit notification that nothing has changed, along with an indication of the next scheduled review date.			
11. The Respondent shall provide access reports from facilities (physical access) down to the individual device level (physical or virtual access), upon request, when a service-impacting issue has occurred. This includes the physical device that the CHE resides on and the components of that device, e.g., the hard drive, power supply etc.			
12. The Respondent shall describe how their solution supports multifactor authentication for any access into the systems supporting this CHE, as well as for access to any externally accessible portals, user interfaces (UIs), system dashboards, etc..			
13. The Respondent shall describe their security software update policy and procedures, for both normal maintenance as well as emergency			

Requirements:	Complies	Does Not Comply	Partially Complies
software patches, antivirus updates, etc., and include the frequency and turnaround time for different types of updates.			
14. The Respondent shall describe their plan/approach for adopting evolving security best practices.			
15. The Respondent shall complete the NG-SEC Audit Checklist, and submit for approval, as described in NENA 75-502, *Next Generation 9-1-1 Security (NG-SEC) Audit Checklist 75-502*. (For this procurement, the Respondent must comply with all requirements designated as Required "R" in column labeled "Compliance Finding").			
16. The Respondent shall 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.			
17. The Respondent shall 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.			
18. The Respondent shall support the ability to isolate specific PSAP sites in case of cybersecurity breach.			
19. If the Respondent is proposing a cloud-based solution, the Respondent shall ensure that System and Organization Controls 2 (SOC 2) compliance is achieved.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

3.4 CHE Network Documentation

The Respondent shall provide the following documentation associated with its proposed CHE solution.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide its proposed network design (transitional and end state [where a statewide ESInet is available], if applicable).			
2. The Respondent shall provide as-built documentation depicting network paths and equipment diversity, prior to acceptance testing of the solution.			
3. The Respondent shall provide network interface specifications for interoperating with CHE, including CHE that is supported by neighboring SRs that may be provided by different SR providers.			
4. The Respondent shall provide detailed as-built solution documentation to include network, equipment, and cloud information (as applicable), including network paths, network providers, BGP information, firewalls, availability zones, software versions, etc.), as well as configured parameters (implemented design).			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

3.5 Monitoring and Alarming

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide physical access monitoring and reporting for all facilities where the software running the call handling service reside.			
2. The Respondent shall provide automated network node and software instance monitoring and alarming in real, or near-real, time.			
3. The Respondent shall provide event logging and reporting in real, or near-real, time.			
4. The Respondent shall provide CHE network monitoring and alerting (regardless of whether the network is new or existing), and to act on the alerts according to the level of impact to the CHE service and in accordance with service level agreements (SLAs).			
5. The Respondent shall provide CHE hardware and software monitoring and alerting and to act on the alerts according to the level of impact to the CHE service and in accordance with service level agreements (SLAs).			
6. The Respondent shall provide user-definable notification levels and recipients with text and email delivery options.			
7. The Respondent shall provide an executive dashboard with (near) real-time updates of alarms, support tickets, and network status.			
8. The Respondent shall provide the ability to replicate select alerts to a third- party monitoring/reporting system.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

3.6 Network Operations Center / Security Operations Center

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide 24 x 7 x 365 staffed Network Operations Center (NOC)/Security Operations Center (SOC) with hot (preferred) or warm backup within North America.			
2. The Respondent shall provide the ability for users to submit, track, and modify tickets by phone, email, and via any direct Information Technology Service Management (ITSM) user access that may be available, for incidents, problems, changes, and maintenance.			
3. The Respondent shall provide outward notifications and updates of customer tickets through phone, email, and text.			
4. The Respondent shall provide fully documented escalation procedures with contact information for all primary and secondary responsible personnel at all levels of escalation.			
5. The Respondent shall provide Reason for Outage (RFO) reports and regulatory compliance reporting in accordance with Federal Communications Commission (FCC) requirements.			
6. Preliminary RFO reports are due to INCOG within five business days of initial report of issue; final root-cause analysis within 14 business days of root cause determination including steps taken to prevent issue from occurring again.			
7. The Respondent shall provide a media contact for any outage or service interruption / failure. INCOG shall be informed immediately of any changes in contact information.			
8. The Respondent shall provide a governance contact for any outage or service failure. INCOG shall be informed immediately of any changes in contact information.			

Requirements:	Complies	Does Not Comply	Partially Complies
9. The Respondent shall provide a service management contact for any outage or service failure. INCOG shall be informed immediately of any changes in contact information.			
10. The Respondent shall provide access to technical and executive staff for escalations.			
11. The Respondent shall provide NOC/SOC staff trained or experienced with 9-1-1 issues with regular refresher/update training plan.			
12. The Respondent shall provide the ability to access and troubleshoot, diagnose, and repair network and systems remotely.			
13. The Respondent shall provide the ability and commitment to support the troubleshooting of all service affecting issues, even when it is determined that the root cause of the issue is outside the scope of the Respondent's solution or service. (e.g., provide call traces and log analysis to assist in troubleshooting a third-party CHE location display issue).			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4 CALL-HANDLING REQUIREMENTS

4.1 Industry Standards Evolution

Requirements:	Complies	Does Not Comply	Partially Complies
1. As industry standards evolve, the Respondent's solution shall be upgraded to maintain conformance with the current version of established industry standards. The Respondent's solution shall support new call-handling and security industry standards within 18 months of ratification of applicable industry standards. Conformance requirements also apply to the supporting standards referenced within each standard.			
2. As solution updates are made to maintain conformance, the solution shall not abandon services, features, or functionality in place at the time of the solution upgrade. The Respondent must divulge and justify any performance or feature changes prior to the upgrade and report them to INCOG for approval.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.2 Regulatory and i3 Standards Conformance

The Respondent's solution shall be an i3-conformant call-handling system that meets regulatory requirements as noted below.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall conform to the latest published/ratified version of NENA STA-010.3e-2021, *NENA i3 Standard for Next Generation 9-1-1*.			
2. The solution shall interface with any NENA i3-conformant NGCS and ESInet.			

Requirements:	Complies	Does Not Comply	Partially Complies
3. The Respondent shall provide the number of its operational call-handling installations that utilize Presence Information Data Format Location Object (PIDF-LO), Emergency Incident Data Object (EIDO), HTTP[3]-enabled location delivery (HELD), Location-to-Service Translation (LoST), Additional Data Repository (ADR) queries, and other i3 protocols.			
4. The solution shall function in a legacy 9-1-1 network environment during the transition to an i3 NGCS and ESInet infrastructure.			
5. The CHE solution shall be capable of receiving and processing 9-1-1 location that meets FCC requirements and timelines regarding horizontal location accuracy and, if supported, z-axis availability and accuracy.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.3 Call-Handling Technical Support

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide a 24 x 7 NOC/SOC for reporting and escalating software and hardware issues. The NOC/SOC Tier 1 and 2 personnel shall be based in North America. The Respondent shall describe how it defines Tier 1 through Tier 4 support.			

[3] *Hypertext Transfer Protocol*

Requirements:	Complies	Does Not Comply	Partially Complies
2. Upon identification of an issue, the Respondent shall adhere to the timelines for response time, repair time, and escalation intervals provided in Appendix A, Section 1.			
3. The Respondent shall provide a redundant/secondary/backup NOC/SOC or equivalent support capabilities and capacity in the event the primary center is offline or otherwise unusable.			
4. The Respondent shall provide onsite technical support to address issues with any vendor-provided hardware or software that may be installed at INCOG facilities. This can include addressing system alarms, fixing a workstation/router/firewall, etc., or troubleshooting a system outage. The onsite technical support shall be in accordance with agreed repair time SLAs.			
5. The Respondent shall allow PSAP personnel to interact with technical support personnel via collaborative tools, such as Zoom, Google Meet, Microsoft Teams, Webex.			
6. The Respondent shall provide a NOC/SOC COOP plan that provides for situations when NOC/SOC staff are unable to work onsite (such as the COVID-19 pandemic environment).			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.4 Solution Validation

Requirements:	Complies	Does Not Comply	Partially Complies
1. At the discretion of INCOG, the Respondent shall allow for independent third-party validation of all mandatory solution requirements and feature functionality prior to cutover of the site(s).			
2. The solution shall provide transparency and access to all SIP messaging, call detail records (CDRs), key performance indicators (KPIs), (e.g., MOS, delay, jitter, packet loss), call logs, and any other data determined to be necessary to verify compliance with contractual obligations or to troubleshoot issues.			
3. The CHE solution shall utilize INCOG's training workstations, which may be on the PSAP floor or in a separate Training room, for integration and smoke testing before executing full acceptance testing at the PSAPs, but also to test bug fixes and new feature implementations, MOP verification, etc. The Respondent shall describe how testing is performed on Training workstations and explain any capabilities available to identify test 911 calls and automatically direct them to a Training user/workstation, based on certain criteria.			
4. The Respondent shall provide documentation of completed results from testing of any hardware or software changes in the training room.			
5. The Respondent shall provide a full test suite that demonstrates traceability to all requirements where compliance was selected within this document for review and approval by INCOG within three months of contract signature. INCOG will review and determine acceptance or modification of test suite.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.5 Multi-Tenant capability

The Respondent's solution shall support partitioning of tenants' (i.e., agencies') call-handling resources.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall deploy multiple tenants as necessary for INCOG's call handling solution to support their Primary, Backup, Training, and potentially other PSAPs, if necessary in the future. INCOG also requires the Training workstations be capable of being used for live 911 call-taking if necessary.			
2. INCOG shall be able to create their own unique set of configurations for each tenant (e.g., agent identifications [IDs], roles, permissions, groups, screen layouts, speed-dial catalogs, management information system [MIS] reports, system status, screen layouts, greetings, etc.).			
3. Authorized INCOG administrative personnel shall have full visibility into the service, including configuration control and reporting, on a per-PSAP basis.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.6 Integrated Text-to-911

The Respondent's solution shall support an integrated Short Message Service (SMS)-based text-to-911 solution via SIP/Message Session Relay Protocol (MSRP).

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall explain how text calls are received, answered, and tracked in the system.			

Requirements:	Complies	Does Not Comply	Partially Complies
2. The Respondent shall explain disposition of attached multimedia and how text calls are handled by the MIS.			
3. The Respondent shall explain how text calls are transferred and shared, as well as any limitations.			
4. The Respondent shall provide examples of the applicable UIs (e.g., screenshots).			
5. The Respondent shall provide the ability to text from 911. The Respondent shall describe any additional features that may be available for text conversations initiated by the PSAP, for example streaming video, images.			
6. The solution shall be able to accept SMS text delivery via ESInet connection (i.e., not require a separate connection for SMS delivery).			
7. The Respondent's CHE solution shall provide for predefined PSAP-defined scripts for use during text call transactions.			
8. The Respondent shall provide SMS foreign language translation capability. The Respondent shall describe how the feature works, including any over-the-top connectivity that may be required, and whether this feature is available today or is a roadmap item for the future.			
9. The Respondent shall support the ability to transfer text messages with conversation history. Please explain how this feature works in the context of your solution.			
10. The Respondent shall provide details regarding transfers between different TCC providers, including text conversation history, and any limitations therein.			

4.7 Real-Time Text

The Respondent's solution shall support real-time text.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall describe plans for supporting Real-Time Text (RTT) to 911 as a part of its solution or explain any plans to offer this feature in the future.			
2. If not currently developed, the Respondent shall provide details of when this capability will be included in the proposed solution as a no-charge upgrade/deliverable.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.8 Transcription and Translation

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall provide the ability to translate the 9-1-1 voice call to a text record or documented dialogue. The Respondent shall state whether this requires an internet connection to a third-party provider. The Respondent shall clearly state whether this feature is available today, or if it is a roadmap item to be delivered in the future, and if costs associated with this feature are included or additional.			
2. The solution shall provide foreign language translation capabilities. Particularly for the languages of Spanish, Korean, Turkish, Russian, Vietnamese/Hmong, Chinese, German, Arabic, Burmese, Romanian, and Portuguese. The Respondent shall describe how the feature works, including any over-the-top connectivity that may be required, and			

Requirements:	Complies	Does Not Comply	Partially Complies
whether this feature is available today or is a roadmap item for the future.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.9 Status Lights

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall be capable of displaying call taker status visually, for example, busy 911 / busy admin-line / available / needs assistance, etc. This can be provided via color schemes on call taker screens or via light poles. The Respondent shall describe their solution.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.10 User Profiles

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide user profile settings, on a per-PSAP basis, which are retained between logins, during upgrades, and between sessions (i.e., logoff and return next day).			
2. The solution shall be capable of establishing skills-based profiles which would allow INCOG to have calls distributed to the appropriate user based on the type of call – wireline, wireless, administrative, etc. The Respondent shall describe this feature and identify any constraints or restrictions.			
3. Profiles shall be stored on the network and be available from any workstation on the same call-handling system.			
4. Access to call-handling assets (e.g., trunks, lines, PSAP-defined queues [including those based on Class of Service/call type, rollovers from another agency, abandoned COOP calls], speed dials, configurations, screen layouts, greetings, etc.) may be controlled by a user's profile.			
5. The Respondent shall provide at least one read-only user profile for users to see configurations and settings, without having the capability to change them.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.11 Redundancy, Reliability, Availability

The Respondent's proposed solution shall satisfy the redundancy, availability, and diversity requirements that follow.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall automatically (i.e., without manual intervention) transfer or failover core processing functionality from one call handling node to another (i.e., "hot" recovery site) upon detection of a problem that impacts the system's ability to meet the 99.999% service level requirement (SLR).			
2. During such an event, call-handling capacity and performance shall not be degraded.			
3. It shall be possible to manually switch core-processing functionality back to its normal operating state, as well as to have the system automatically recover and resync once a problem is corrected.			
4. The Respondent shall provide a detailed description of how the solution achieves 99.999% availability.			
5. Core-processing functionality may be distributed across two or more call-handling datacenters provided by the Respondent and/or INCOG.			
6. Each call-handling datacenter shall have sufficient configured capacity to support 125% of busy-hour 911 call volume and call-mapping functionality for all ECCs served by that call-handling system.			
7. The solution shall support remote call-taking capability via virtual private network (VPN) connections over the public internet or other broadband connection via Respondent-provided (and supported/maintained) laptops. The Respondent shall explain their available solutions.			
8. The Respondent should describe the solution's hot-seating capabilities (i.e., the ability for a telecommunicator from one ECC or agency to login at a workstation at a different ECC or agency and process calls, provided both ECCs/agencies are co-tenants on the same system, and have their "home" assets [e.g., trunks, lines, queues, speed dial lists, screen layouts, map, greetings, etc.] available at the other ECC).			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.12 Security

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall comply with NENA-STA-040.2-2024, NENA Security for Next-Generation 9-1-1 Standard (NG-SEC). The Respondent shall detail how its solution addresses the requirements of the following sections of the standard:			
a. 6.2 - Access Control			
b. 6.3 – Device Connectivity			
c. 6.7.1 - Remote Access Device Security			
d. Section 6.17 - Remote Access			
2. The Respondent shall describe CHE security software update policy, frequency, and procedures (include frequency of antivirus updates).			
3. The Respondent shall describe policy/approach to independent system security audits.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.13 Long-term Availability

The Respondent shall commit to long-term availability.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide 12 months' (minimum) advance written notification to INCOG for any end-of-life (EOL) or end-of-support (EOS) component, with a plan for how the affected component(s) will be replaced without affecting service.			
2. The proposed solution shall be supported by the manufacturer(s) for a minimum of five years (plus any optional contract extensions) from the date of full system acceptance by INCOG.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.14 CAD Interoperability

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall support the computer-aided dispatch (CAD) system interface as described in NENA-STA-027.3-2018, *NENA E9-1-1 PSAP Equipment Standards*.			
2. The solution shall support NG9-1-1 functionality that includes the delivery of Additional Data, including text, imagery, and video conveyed in an Emergency Incident Data Object (EIDO) "by value" or "by			

Requirements:	Complies	Does Not Comply	Partially Complies
reference" to the CAD system (or NG9-1-1 functional equivalent). The NG9-1-1 CAD system shall be capable of rendering multimedia received via Additional Data, including audio, video, imagery, and text. EIDOs shall be formatted as defined in NENA-STA-021.1-2021, *NENA Standard for Emergency Incident Data Object (EIDO)*. The interface used for EIDO conveyance should align with NENA-STA-024.1b-2023, *NENA Standard for the Conveyance of Emergency Incident Data Objects (EIDOs) between Next Generation (NG9-1-1) Systems and Applications*. If the EIDO conveyance interface described in NENA-STA-024.1b-2023 is not supported, please describe any proprietary APIs that are available with your solution to support the conveyance of EIDOs between your CHE solution and CAD.			
3. The solution shall support both serial and IP-based connections.			
4. The solution shall support a bi–directional interface with the CAD system.			
5. The Respondent's solution shall detail the process to import and export phone book data from the CHE into CAD and vice versa.			
6. The solution shall support CHE to CAD cut/paste feature and describe how this functionality will be enabled.			
7. The Respondent shall explain any capabilities available to resync call information with CAD systems if the CAD is down or the connection is lost for a period of time. Respondents shall explain how the resync is controlled – automatically, or manually.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.15 Recording/Instant Recall Recorder Interoperability

Requirements:	Complies	Does Not Comply	Partially Complies
1. The CHE solution shall log all media associated with emergency calls. The CHFE must support the logging of the media associated with all other calls received on any designated queue based on local capture policy.			
2. The CHE solution shall support storage of audio, video and images.			
3. The Respondent shall describe mechanisms used for remote recording and storage of PSAP audio, video or images.			
4. The CHE solution must support the logging of the media of all calls received or placed by a particular Agent, including media received from the Agent's microphone and media sent to the Agent's earpiece, or text or video sent or received.			
5. The CHE solution shall support an Instant Recall Recorder that allows for the quick review of current or recent emergency communications content consisting of all media types. The CHE solution shall allow flexibility in the recalled communications presented to the PSAP (e.g., limiting recall to communications the user has handled, to specific communications types, and/or limiting the time period from which recent communications can be recalled) based on local policy. The Instant Recall Recorder capability provided by the CHE solution shall allow the user to navigate within and between recalled communications.			
6. The solution shall support recording at workstations for both radio and telephony.			
7. The solution shall support playback of radio and 911 calls independently or together.			

Requirements:	Complies	Does Not Comply	Partially Complies
8. The solution shall support the following with single-click playback controls that enable the user to navigate to any portion of the recorded conversation(s): a. Play. b. Pause. c. Stop. d. Play forward/fast forward (without altering voice pitch). e. Rewind. f. Repeat. g. Skip forward or back a configurable number of seconds.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.16 PSAP/ECC Hardware

Requirements:	Complies	Does Not Comply	Partially Complies
1. PSAP/ECC hardware (e.g., monitors, keyboards, mice, headsets, phones) must be new and covered by (extended) manufacturer warranty for no less than five years from the date the device is placed into operation, if not provided by the PSAP/ECC.			
2. Whenever supported by the device manufacturer, all servers, switches, routers, firewalls, and other devices within the solution shall be configured with redundant power supplies and redundant network interfaces.			

Requirements:	Complies	Does Not Comply	Partially Complies
3. The Respondent shall work with INCOG to provide (and maintain) mobile laptop call-taking positions and spares at each PSAP to be used for remote call processing.			
4. The Respondent's proposed CHE solution shall provide a headset interface that allows the call-taker to plug in to the vendor's CHE and converse with callers. The headset interface shall include a volume control. The interface shall provide audio outputs to interface to the PSAP audio enclosure used to combine radio and telephone audio into one headset. Describe how wireless headsets are secured (i.e., what encryption is used with Bluetooth)			
5. The Respondent's proposed CHE solution shall provide an external keypad used for dialing telephone numbers, answer/release, volume control and other telephone functions.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.17 Location Information Server/Location Database

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution should support interface(s) with the Location Information Server (LIS) as defined in NENA-STA-010.3e-2021, *NENA Detailed Functional and Interface Standards for the NENA i3 Solution*, and the Location Database (LDB) as defined in NENA-INF-008.1 (previously			

Requirements:	Complies	Does Not Comply	Partially Complies
NENA 77-501), *NENA NG9-1-1 Transition Plan Considerations Information Document*, (or their successor documents, once published).			
2. The Respondent should describe how the proposed solution will address any transition period, during which both legacy Automatic Location Identification (ALI) services and LDB and/or i3-compliant LIS services may need to be accessed by the Respondent's call-handling solution.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.18 Additional Data/Emergency Incident Data Object (EIDO)

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall support a SIP interface from the ESInet/NGCS that includes Additional Data conveyed "by reference" and "by value".			
2. The solution shall support interface(s) with Additional Data Repositories (ADRs) as defined in NENA-STA-010.3e-2021, *NENA Detailed Functional and Interface Standards for the NENA i3 Solution*, (or its successor document, once published) to facilitate the dereferencing of Additional Data that is conveyed "by reference".			
3. The solution should support the creation EIDOs as defined in NENA-STA-021.1-2021, *NENA Standard for Emergency Incident Data Object (EIDO)* (or its successor document, once published), and the conveyance of EIDOs "by value" and "by reference" between functional			

Requirements:	Complies	Does Not Comply	Partially Complies
components of the solution, and “by reference” between PSAPs/agencies during call transfer.			
4. The solution should support an HTTPS[4] GET interface to facilitate the dereferencing of EIDOs that are received “by reference”.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.19 Human-Machine Interface (HMI)

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall comply with NENA 54-750, *NENA/APCO Human Machine Interface & PSAP Display Requirements*, and provide an explanation of any areas of non-compliance with the standard.			
2. If a call is default-routed or otherwise diverted to a destination other than the normally intended destination, the call-handling solution shall recognize and present the originally intended destination and the reason why the call was diverted, as indicated in the SIP History-Info Header, and the associated Reason Parameter. This may take the form of a visual indication to the call taker as described in Section 3.3.CC of NENA 54-750.			

[4] HyperText Transfer Protocol Secure

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.20 Distinctive Ring Tones

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall provide the ability to configure distinctive ring tones for 911 calls, 911 calls in a pending queue, administrative calls, and text messages.			
2. The solution shall provide the ability to configure any of the call types (911, 911 pending, admin, text, etc.) with distinctive ring tones both audibly and via in-ear headsets.			
3. The solution shall support user-selected, distinctive ring tones for each Automatic Call Distribution (ACD) queue or call type.			
4. The solution shall provide distinctive ring tones to be customized by agent role or login.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.21 Call Transfer

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent's solution shall be capable of detecting a request for an emergency call transfer and providing the signaling and procedures described in Section 4.7.1 of NENA STA-010.3e-2021, *Detailed Functional and Interface Specifications for the NENA i3 Solution,* to support an attended transfer by: a. Establishing a conference (if not already established) with a conference bridge in the serving ESInet b. Referring the emergency caller to the conference c. Referring the transfer-to party to the conference d. Completing the transfer			
2. The solution shall support initiation of a blind transfer following the signaling and procedures described in Section 4.7.2 of NENA STA-010.3e-2021, *Detailed Functional and Interface Specifications for the NENA i3 Solution.*			
3. When transferring an emergency call, the solution shall support the ability to pass the location of the original caller, as well as any Additional Data that the transferring PSAP call taker may have received during the processing of the emergency call or was generated by the call taker as a result of processing the incoming emergency call, in an Emergency Incident Data Object (EIDO). The EIDO shall be sent "by reference" following the procedures described in Section 4.7.4 of NENA STA-010.3e-2021, *Detailed Functional and Interface Specifications for the NENA i3 Solution*.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.22 Conference Controller

The Respondent shall support the conferencing capabilities that follow.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The conference controller shall enable the telecommunicator to add an outside caller or inside caller to an in-progress “live” call while remaining on the line, with no limitation as to what type of call the telecommunicator is handling.			
2. The conference controller shall automatically control the audio levels (AGC) of the calling parties so that no degradation of voice quality occurs.			
3. The original telecommunicator shall be able to mute/unmute (i.e., disable/enable the microphone of) any party on the conference.			
4. The original telecommunicator shall be able to disable/enable the earpiece/speaker of any party on the conference without muting that party’s audio (i.e., allow the telecommunicator to speak to others on the conference, without that party hearing, while still able to hear that party).			
5. The original telecommunicator shall be able to select and drop any party from the conference.			
6. The original telecommunicator, or any of the conference parties, shall be able to drop out of the conference without disconnecting the original caller.			
7. The conferencing feature shall support, at a minimum, any combination of up to eight parties.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.23 Call Monitoring

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall allow authorized PSAP/ECC personnel to listen quietly to another telecommunicator's live conversation.			
2. The monitoring feature shall be controlled by the authorized personnel's credentials.			
3. Monitoring shall include an option for the telecommunicator being monitored to be made aware (visually or audibly) when their call is being monitored.			
4. Monitoring shall not degrade the audio quality of the call.			
5. The Respondent shall describe its options, or plans, for supporting call-monitoring-like functionality for text-to-9-1-1 sessions.			
6. The Respondent shall describe its ability to allow authorized personnel to post temporary notifications on call-taker screens, (i.e. "bill-boarding"), without blocking screen real-estate that could contain critical information, if required by the PSAP.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.24 Call Barge-In

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall allow authorized PSAP/ECC personnel to listen quietly and mute/unmute (barge-in) while listening to another telecommunicator's live conversation.			
2. The solution shall allow the feature to be activated by utilizing a mouse or an easily invoked keyboard command.			
3. This feature shall not degrade the audio quality of the call.			
4. This feature shall be configurable to provide a tone to announce the barge-in.			
5. Th solution shall allow a telecommunicator or supervisor using this feature to become part of a three-way call with the caller and original telecommunicator.			
6. The Respondent shall describe options or plans for supporting a barge-in-like capability for text-to-911 sessions.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.25 Callback

The Respondent's solution shall support the callback capabilities that follow.

Requirements:	Complies	Does Not Comply	Partially Complies
1. Callback of any 911 “call” (i.e., wireline, wireless, telecommunications device for the deaf/teletypewriter [TDD/TTY], text, and Voice over IP [VoIP] callers) shall be based on the calling party number associated with the emergency caller.			
2. The solution shall utilize the calling party number (CPN) of a 911 caller to invoke the callback process and should automatically recognize +1 calls.			
3. The solution shall identify callback calls by including an indication of “psap-callback” in the SIP signaling (i.e., the SIP Priority header), as described in RFC 7090.			
4. The solution shall use the Caller ID (CID) information to allow a callback to an administrative caller.			
5. Any required dialing prefix digit(s) insertion/deletion (e.g., adding +9 or removing the area code) shall be automatic and not require manual input.			
6. The callback function shall require only a single mouse click.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.26 Abandoned Calls

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall provide a visual and audible indication for abandoned calls.			
2. The solution shall display the number of abandoned calls from the same callback number and allow a single successful callback to clear all displayed entries from the same callback number.			
3. The solution shall clear the abandoned call count display upon successful callback and answer of the telephone number.			
4. The solution shall provide a configurable option allowing for an automatic response to an abandoned call.			
5. The solution shall provide each individual agency with the ability to configure the automatic-callback option to be enabled or disabled by the agency.			
6. The solution shall allow the system to automatically attempt to return a call and/or text message to an abandoned call, and to prompt the recipient of the call to take an action (e.g., press 1 to notify the agency that no assistance is needed; press 2 to be routed to 911).			
7. The solution shall provide abandoned call reports as part of its MIS.			
8. The solution shall support the capability to allow a PSAP that would have received a call to receive a notification indicating that the call was started, but then cancelled prior to the PSAP responding to SIP call setup signaling associated with the call (i.e., an Abandoned Call event occurred).			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.27 Repeat Callers

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall provide a caller history feature that displays the date and time of the last 50 to 100 previous calls from the same number and include notes provided by the telecommunicator(s) who handled the previous calls.			
2. The solution shall identify the repeat-call condition to the telecommunicator.			
3. The solution shall allow agencies to specify that new calls from the same caller (within a configurable period of time) shall be routed to the same telecommunicator who handled previous call(s), if that telecommunicator is available.			
4. The Respondent shall describe capabilities for identifying and managing abusive repeat callers (e.g., non-service initialized [NSI] wireless phones, telephony denial of service [TDoS], location).			
5. The Respondent shall describe system capability to allow call history printing from a snapshot as well as to retrieve printable call history reports. Advise how long call history data will be available for access/reference by INCOG.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.28 Call Spike/Major Incident Call Volume Screening/Call Prescreening

Requirements:	Complies	Does Not Comply	Partially Complies
1. Respondent shall describe support for feature functionality that enables the PSAP to segregate 9-1-1 calls being generated by an incident at a specific geographic location.			
2. Respondent shall describe any queueing ability to move said calls to a separate queue.			
3. Respondent shall describe any auto answer, auto attendant announce ability to provide instructions of notice related to the incident.			
4. Respondent's system will have a feature allowing the caller to select a button number to further handle the caller's call.			
5. Respondent shall describe support for feature functionality that allows for a virtual attendant to prescreen incoming 9-1-1 or non-emergency calls, and based on caller responses, forward the call to a 9-1-1 queue, an administrative report line, or other proposed position.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.29 Real-time Queries

Requirements:	Complies	Does Not Comply	Partially Complies
1. Telecommunicators shall have the ability to query the call-handling system with 10-digit numbers, both pANIs and callback numbers, along			

Requirements:	Complies	Does Not Comply	Partially Complies
with a date/time range, to retrieve information received from those numbers, for both 911 and non-911 calls.			
2. Telecommunicators do not have to be on an active 9-1-1 call to retrieve this information.			
3. Respondents shall explain their ability to pin any recorded voice conversations to the query response, allowing PSAP personnel greater efficiency in their investigations.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.30 Speed Dials

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall provide separate and multiple speed-dial lists for each group: a. System wide (all tenants). b. ECC/Agency (local operations); and c. Personal (by role or login ID).			
2. The system administrator shall be capable of maintaining the enterprise-wide speed-dial list, while individual ECC/Agency speed-dial lists can be managed by the local ECC system administrator.			

Requirements:	Complies	Does Not Comply	Partially Complies
3. Telecommunicators shall have the ability to create/maintain their own personal speed-dial lists. The ECC/Agency should have the capability to turn off personal speed-dial lists.			
4. The solution shall provide access to speed dials with a minimum of mouse click actions.			
5. The solution shall provide a hierarchical organization of speed dials (up to at least five levels deep), in which a list entry may refer to a single speed dial or another list.			
6. The solution shall allow alphanumeric entries, e.g., 1-888-911-HELP.			
7. The solution shall allow the extra digits or codes necessary to automatically dial a number and complete a call based on line type (e.g., long distance access, personal identification numbers [PINs], and star-code transfers).			
8. Telecommunicators shall not need to take any action to immediately access speed-dial list changes.			
9. The solution shall associate content (files, links, etc.) with a speed-dial entry to include images, video, floorplans, comments, etc. The Respondent shall describe if and how this content is searchable.			
10. The solution shall allow display of speed dials in either list form or graphical form (i.e., as a grid of clickable buttons, icons, graphics, and/or images).			
11. When a speed dial or list is assigned to a button that appears in the telecommunicator UI, the solution shall allow for the display (in a popup window) of a user-selectable set of fields when the mouse pointer hovers over the button.			
12. The Respondent shall describe how additional information is entered and associated with an entry.			

Requirements:	Complies	Does Not Comply	Partially Complies
13. The Respondent shall describe search functionality (search-as-you-type capability preferred).			
14. The Respondent shall describe options for uploading and using user-provided icons/graphics/images for speed-dial buttons.			
15. The Respondent shall support speed-dial entries/buttons that are dynamically populated with agencies (e.g., law enforcement, fire/rescue, emergency medical services [EMS], poison control, animal control) and services (e.g., towing, etc.), based on the caller's location.			
16. The solution shall support a minimum of ten speed-dial entries per service area (analogous to a legacy emergency service zone [ESZ]).			
17. The solution shall support intelligent manipulation of the dialed digits (e.g., area code removal for 7-digit local dialing, adding '+1' for 11-digit dialing, etc.).			
18. The Respondent shall describe all methods of speed-dial import and export (e.g., comma-separated values [CSV], Structured Query Language [SQL], XML, etc.).			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.31 Automatic Call Distribution

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall permit trained and authorized INCOG staff (by role) to provision ACD-related queues, routing, and telecommunicator skill settings, as needed.			
2. The solution shall support, at a minimum, the following ACD next-available-telecommunicator selection algorithms on a per-queue basis, and the algorithm shall honor any role-based limits that may be configured (like new hires only receiving non-emergency calls):			
a. Longest idle.			
b. Top down.			
c. Round robin.			
d. Ring all.			
3. The solution shall provide the ability to queue based on call-type, (wireline, wireless, VOIP, text, etc.).			
4. The solution shall provide the ability to change roles without having to log out and log back in.			
5. The solution shall display to a telecommunicator the number of calls in each queue.			
6. The solution shall toggle between “ready” and “not ready.” While ready, telecommunicators can receive calls presented through the ACD queues. Similarly, ACD calls are not presented to telecommunicators who are not ready.			
7. The solution shall provide the option to require a telecommunicator to select from an agency-defined list of reasons when changing their status to “not ready.”			
8. In a “longest idle” ACD environment, switching to “not ready” shall not reset the timer used to determine “longest idle” status.			

Requirements:	Complies	Does Not Comply	Partially Complies
9. The solution shall provide a configurable option of forced (automatic) answer of ACD calls, which connects 9-1-1 callers to the next available telecommunicator, without any action needed on the part of the telecommunicator. Optionally, forced answer can provide an audible alert to the telecommunicator prior to connecting the 9-1-1 caller to the telecommunicator.			
10. The solution shall provide an optional, automatic, and configurable "wrap up" period following the end of a call. During this period, the telecommunicator is considered unavailable for ACD calls and may perform post-call tasks without interruption. Once the wrap up period expires, the telecommunicator is automatically made available for ACD calls.			
11. The solution shall support the ability of each telecommunicator to record automatic greetings, in their own voice, for each queue or call type (wireline, wireless, admin, text, etc.). This enables consistent call answering, as well as giving the telecommunicator a notification of the type of call they are about to handle.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.32 Real-time Statistics

Requirements:	Complies	Does Not Comply	Partially Complies
1. The solution shall provide an option for one or more wall-mounted monitor/television displays for presenting real-time call information as configured by the PSAP/ECC.			
2. Display information shall include, at a minimum:			
a. Name of queue or call type/category (wireline, wireless, text, etc.).			
b. Number of calls in queue or call type/category.			
c. Longest call-in queue or call type/category.			
d. Number of telecommunicators logged in.			
e. Number of telecommunicators available for calls.			
f. Number of telecommunicators not ready.			
3. The Respondent's CHE solution shall support the ability to add call location notes based on address or phone number.			
4. The solution shall support configurable thresholds for color and audible alerts.			

An example of the display that's used today is shown below.

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.33 Call Mapping

In the event that the Respondent's call-handling solution does NOT include call location mapping as a no-charge feature included in the base version of its solution, the Respondent is asked to provide separate pricing for a call location mapping solution, optionally available on a per-PSAP basis, that is fully integrated with the call-handling solution, and which meets the requirements below.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The mapping solution shall allow for the installation and display of GIS map layers provided by INCOG, e.g. fire hydrants, street cameras, AED devices, etc.			

Requirements:	Complies	Does Not Comply	Partially Complies
2. The map shall display ***emergency event*** location and ***calling device*** location information.			
3. Map display configuration (e.g., map scale, base map data, iconography, caller/event location display rules) shall be determined by the user's profile/role.			
4. The map shall display updated location (from CHE re-bids) in real time.			
5. The map shall display z-axis location data received by value or reference.			
6. The map shall display the z-axis uncertainty and accuracy estimates.			
7. The mapping solution shall convert 3D (x, y, z)-axis information back to 2D (x, y) data if required for the CAD (sometimes known as flattening).			
8. The mapping solution shall implement the requirements specified in NENA-REQ-003.1-2022, *NENA Requirements for 3D GIS for E9-1-1 and NG9-1-1*, including implementing "fallback" to 2D capabilities for queries to any ECRF that does not have 3D support.			
9. The mapping solution shall provide the ability to accept or reject the updated location results.			
10. If previous calls/incidents are shown on the map, it shall provide the ability to configure how long those calls/incidents remain on the display before being automatically removed/hidden.			
11. The map shall provide the ability to draw and label, modify, and delete geometric shapes and points on the display.			
12. The mapping solution shall provide the ability to make such dynamic features private (i.e., visible only to the creating agent), visible to specific groups (i.e., roles, agencies), or visible to all users.			

Requirements:	Complies	Does Not Comply	Partially Complies
13. Dynamic features shall be able to be captured and stored for easy reuse.			
14. Users shall have the ability to “zoom” the map display, in and out.			
15. Zoom parameters (e.g., default zoom level when call arrives; appearance of various features, information, iconography, and layers at different zoom levels) shall be configurable based on user role.			
16. Zoom history shall make it possible to return to the previous zoom level with a single click (up to ten steps back).			
17. It shall be possible to return to the default zoom level with a single click.			
18. The map shall provide the capability to pan the display.			
19. Pan history shall make it possible to return to the previous pan location with a single click (up to ten steps back).			
20. It shall be possible to return to the current call location with a single click.			
21. The mapping solution shall provide the ability to configure default Geographic Information System (GIS) layers that are visible based on user login/role, and to allow users to manually select/unselect individual GIS layers for display.			
22. The map shall provide the ability to search for a location using either: a) geo-coordinates, b) civic addresses, or c) common place name.			
23. The map shall display location search results to the call-taker.			
24. If multiple results are returned from a location search, each shall include a confidence/match-score and clicking on a result shall re-center the map on the selected location.			

Requirements:	Complies	Does Not Comply	Partially Complies
25. The map shall provide the ability for users to retrieve location information (i.e., address and geo-coordinates) by clicking on a point on the map display.			
26. The map shall provide the ability for users to designate a location as a call/incident location by clicking on a point on the map or selecting it from the list of search results.			
27. The map shall display the emergency response agencies associated with a ***caller's location***.			
28. The map shall display the emergency response agencies associated with an ***emergency/incident location***.			
29. The map shall provide the ability to display the accuracy/uncertainty associated with a given calculated position.			
30. The map shall support the ability to represent calls on the map with different icons based on class of service/type of call (e.g., wireline, wireless, VoIP, SMS).			
31. The map shall support the ability to represent additional location information for a call based on call type/class of service (e.g., wireless, SMS, VoIP).			
32. The map shall display the location of incoming calls to call-takers and provide the ability for call-takers to "cherry pick" the calls they want to answer from the map.			
33. The Respondent shall describe how its solution integrates INCOG GIS data with RapidSOS and Rapid Deploy on the same map display.			
34. The Respondent shall describe the process for updating map data and aerial imagery.			

Requirements:	Complies	Does Not Comply	Partially Complies
35. The solution shall integrate Google or other platforms that provide street-level views.			
36. The solution shall support a CAD interface to import call location data and unit AVL tracking on a per-PSAP basis.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.34 Training

Requirements:	Complies	Does Not Comply	Partially Complies
1. Proposals shall include options for both train-the-trainer and end-user models with different training content for telecommunicator staff versus supervisors and/or administrators.			
2. Operational training on the call-handling and mapping features and functionality will be provided to all telecommunicators and superusers.			
3. Training for superusers shall also include monitoring, reporting, system health, and performance (MIS).			
4. Training for superusers shall also include GIS and mapping administration.			

Requirements:	Complies	Does Not Comply	Partially Complies
5. Respondents shall include options for PSAP/ECC-specific training and train-the-trainer instruction for INCOG training personnel.			
6. Training schedules shall accommodate 24 x 7 shifts.			
7. All training materials shall be available in digital form.			
8. INCOG reserves the right to record all training sessions and make available to staff online for refresher and new-agent training at no additional charge.			
9. Training services shall include an onsite trainer/coach for a minimum of four hours for each different shift immediately following cutover (on-the-job training/coaching).			
10. The Respondent shall provide a summary/syllabus and duration of each training class so that the PSAP/ECC can coordinate personnel schedules.			
11. Training materials shall include quick-reference guides for call-takers (CHE and mapping).			
12. Training for call-takers shall take place no more than one week prior to go-live (retention issues).			
13. The Respondent shall describe the suite of training classes available, including in-person and online options.			
14. INCOG technician certification training (at the manufacturer's site) for two people in two different sessions on different days shall be provided.			
15. INCOG technician training shall include refresher (or new technician) training every two years for the same number of personnel.			

Requirements:	Complies	Does Not Comply	Partially Complies
16. The Respondent shall provide up-to-date on-line training tools available after go-live.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.35 MIS

Requirements:	Complies	Does Not Comply	Partially Complies
1. Authorized personnel shall be able to run reports.			
2. The Respondent's solution shall include the ability to run reports on an individual user's performance.			
3. The PSAP/ECC shall be provided with a business-grade color network printer for printing reports from the MIS.			
4. Reports shall support color charts and graphs.			
5. Authorized personnel shall have the ability to query the data to create and print ad hoc reports.			
6. The Respondent shall provide documentation on the following: a. All built-in reports included in the proposal. b. All additional reports currently available for an additional fee. c. Options available for custom report creation by the manufacturer.			

Requirements:	Complies	Does Not Comply	Partially Complies
d. Options for supplementary training for PSAP/ECC personnel on ad hoc report development. For each report, the Respondent shall include a description as well as an anonymized sample to show the report's layout.			
7. The Respondent's MIS documentation shall include a data dictionary and explanations of data fields available for reporting.			
8. After ad hoc reports have been developed, the solution shall have the ability to save the ad hoc report as a template and to optionally schedule the report for automatic execution.			
9. The solution shall provide for reports to be scheduled for output to files, printers, or other network locations.			
10. The Respondent shall describe how/if its solution can support ECaTS-type reporting for INCOG and generate reports for categories of calls such as misrouted and on-hold calls. The Respondent shall describe what reports are available.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.36 Project Management and Progress Reports

Requirements:	Complies	Does Not Comply	Partially Complies
1. Prior to contracting with INCOG for call handling, the selected Respondent will provide a ***high-level*** project plan that shows the timeline for the entire project starting at contract signature, the Respondent's resources and their associated roles, responsibilities, and resumes, (INCOG reserves the right to refuse resources), and the expectations of INCOG.			
2. The Respondent shall provide a certified project manager to lead the implementation of the Respondent's solution.			
3. INCOG 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.			
4. Examples of what shall be included in the project plan, at a minimum, include:			
a. Data gathering.			
b. PSAP/ECC onsite testing.			
c. Core component installation and testing.			
d. PBX[5]/CHE/mapping and workstation installation.			
e. Gateway/network interface testing at all PSAP/ECC locations.			
f. Location format, update, and discrepancy reporting mechanisms, and interface testing.			
g. Tracking of MSAG/ALI data migration and GIS data uploads with a minimum match rate of 98% between the GIS road centerlines and legacy MSAG/ALI data to achieve i3 readiness.			
h. CAD, logging recorder, analog, digital, and IP voice testing.			

[5] *Private Branch Exchange.*

Requirements:	Complies	Does Not Comply	Partially Complies
i. Comprehensive test and acceptance plan for all network connections verifying complete functionality with the CHE solution.			
j. An overview of the approach and typical steps taken to ensure continuity of PSAP/ECC operations throughout the project.			
k. Respondent's assigned Project Manager shall provide a Gantt chart project plan			
5. Within 30 days of contract signing, the selected Respondent will provide a ***detailed*** project plan, timeline, and schedule, to the contracting ECC/agency and to INCOG. This plan shall include the specific approach and steps to be taken to ensure continuity of ECC operations throughout the project.			
6. The selected Respondent shall facilitate biweekly project calls, (changed to weekly for the last couple of months during acceptance testing and cutover planning), followed by a written progress report, distributed within 24 hours of the call, that captures the minutes and action item updates from the prior project call.			
7. Customer billing shall be accurate and in accordance with the agreed upon schedule. Please describe your process for resolution of billing disputes.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.37 Systems Integration

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall coordinate and work with the appropriate vendors' technicians for the test and turn-up of CAD, recorder, mapping, radio, and local PSAP/ECC telephone system interfaces, as needed.			
2. The Respondent shall integrate local administrative lines (analog or SIP-based) into the CHE solution. The Respondent shall describe the method used for incorporating administrative lines, porting to the Respondent's solution, and adding outgoing lines.			
3. The Respondent shall coordinate and work with OK911MA's ESInet/NGCS vendor for system integration and testing. The Respondent's CHE solution shall support interconnection with OK911MA's ESInet/NGCS, once available, at no additional cost.			
4. The Respondent shall describe any experience or integration capabilities it has with RapidSOS, RapidDeploy, What3Words, Prepared911, and Rave. Further, the Respondent shall describe capabilities that support integration with telematics systems, Real Time Crime Centers, and the radio log module of the Offender Data Information System (ODIS). It is preferred that these applications integrate into the CHE and not require their own, separate, display monitor(s).			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.38 Change Management

Respondent's change-management process must include the following:	Complies	Does Not Comply	Partially Complies
1. Documented change-management process including system and scope changes, team member changes, as well as scheduled and emergency changes			
2. A Method of Procedure (MOP) with backout plan for review by INCOG a minimum 72 hours prior to planned maintenance activities			
3. A means for INCOG to request changes and receive updates on progress			
4. Defined backup procedures			
5. The ability to rollback to a previous version if there is an issue with update/change procedures.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.39 Change Orders

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall submit all change orders in writing.			
2. All change orders require approval by INCOG prior to performing work, not only those for equipment or services not covered under the contract.			
3. INCOG will not accept change orders resulting in additional costs unless additional features are requested by INCOG.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.40 Service Interruptions and Facility Damages

Requirements:	Complies	Does Not Comply	Partially Complies
1. As the selected Respondent performs the installation and cutover of the equipment/services, the Respondent shall ensure that the PSAP/ECC will experience minimal interruption to normal business operations.			
2. Prior to any PSAP/ECC visit, the Respondent shall provide advance notice to, and obtain authorization from, INCOG, which reserves the right to alter or suspend the intended schedule for any reason at its sole discretion.			
3. The Respondent shall be responsible for the repair or restoration of any damages or outages caused by the Respondent, its subcontractors, or delivery personnel to any PSAP/ECC or agency facilities through the receipt, delivery, installation, or testing of the solution.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.41 Storage, Staging, Delivery, and Inventory Control

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall be accountable for the storage of materials until such time that the items are to be installed.			
2. Neither INCOG nor INCOG PSAP/ECC facilities may be used as a warehouse for uninstalled equipment.			
3. The Respondent shall coordinate with INCOG for the shipping, staging, and testing of all equipment prior to installation.			
4. The Respondent shall be responsible for ensuring that the equipment is fully staged, configured, and tested prior to delivery to INCOG.			
5. The Respondent shall arrange for equipment to be delivered onsite as-needed, and the cost for delivery shall be included in the Respondent's proposal.			
6. Receipt, inventory, and movement of material are the responsibility of the Respondent.			
7. The Respondent shall be responsible for the disposal of shipping material, as well as the daily removal of other refuse.			
8. The Respondent shall provide INCOG with a detailed inventory of all equipment installed on PSAP/ECC premises.			
9. At a minimum, the inventory data shall include where it is installed, manufacturer, part number, serial number, quantity, and model number.			
10. The Respondent shall provide the inventory in hard- and soft-copy format using Microsoft Excel.			
11. The Respondent shall be responsible for all hardware, from its receipt prior to staging until it is accepted by PSAP personnel in writing.			

Requirements:	Complies	Does Not Comply	Partially Complies
12. Any hardware or equipment lost, misplaced, or damaged prior to acceptance will be replaced at the Respondent's sole expense.			
13. Designated INCOG technicians shall participate in the deployment of positions at PSAP facilities. During installation of all equipment, the Respondent shall coordinate with INCOG staff and allow any asset tagging and/or labeling to occur, as deemed appropriate by INCOG staff.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.42 Code Compliance, Grounding, and Transient Voltage Surge Suppression

Requirements:	Complies	Does Not Comply	Partially Complies
1. Installation must comply with all applicable national, state, and local codes.			
2. All metallic circuits (data or voice), if any, shall be equipped with both primary and secondary transient voltage surge suppression (TVSS) devices per industry standards and best practices for telecommunications equipment.			
3. The secondary TVSS device shall have an operational indicator in the form of a light or audible signal to alert maintenance personnel that the device has been exercised, failed, or the circuit is no longer protected.			

Requirements:	Complies	Does Not Comply	Partially Complies
4. The PSAP/ECC where TVSS devices are installed shall be provided an onsite spares kit to assist in emergency restoration.			
5. TVSS equipment shall comply with UL 497A, *Secondary Protectors for Communications Circuits.*			
6. Describe the power requirements (voltage, wattage) for the proposed equipment (CHE and backroom equipment)			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.43 Pre-Cutover Acceptance Criteria

Prior to cutover, the Respondent shall provide the documentation that follows.

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide evidence of the backup of all configuration files and databases for all customer-premise-installed equipment.			
2. The Responder shall provide confirmation and documentation of control, monitoring, and alarm solutions.			
3. The Respondent shall provide an inventory of all Respondent-provided, INCOG premise-installed equipment to include manufacturer, model, part number, quantity, serial number, and installed location.			

Requirements:	Complies	Does Not Comply	Partially Complies
4. The Respondent shall provide Acceptance Test Plans (ATPs) and documentation reviewed and approved by INCOG.			
5. If, during testing, INCOG staff believes that a solution test fails, it will provide the Respondent with a written description of what test failed and why. The Respondent will work expeditiously to resolve the problem, providing an estimated time of resolution.			
6. The Respondent shall provide final as-built drawings (preferably in editable Visio format), system-wide and on an individual PSAP basis, within 30 days of cutover.			
7. As-built documentation shall include all customer-premise-installed cabling, equipment, and configurations, bringing attention to unique or special deployment details.			
8. The Respondent shall provide a checklist that includes all items identified in this response and contract. This checklist will be evaluated prior to go-live.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.44 Cutover Coordination

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall coordinate cutover activities with all service providers and INCOG personnel.			

2. A detailed cutover plan, along with coordination conference calls and supporting documentation, shall be provided to all participating parties, at least 45 days before cutover begins.			
3. The Respondent shall review the final cutover plan with INCOG staff at least 14 days prior to cutover.			
4. The 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. The Respondent shall offer the option of in-person, onsite cutover support for end users to ease the transition to the new system. This shall include at least four hours following cutover.			
6. The Respondent shall state the length of time technical support staff will be onsite for each cutover.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.45 Call-Handling Acceptance Testing

Requirements:	Complies	Does Not Comply	Partially Complies
1. INCOG's call-handling acceptance testing is intended to validate that the Respondent's solution functions as expected in the PSAP/ECC environment and as asserted in their response. The testing period shall be sufficient to demonstrate the solution's functionality, performance and reliability (i.e. failover). The acceptance testing period shall occur no more than 30 days prior to PSAP/ECC cutover and must not have any			

Requirements:	Complies	Does Not Comply	Partially Complies
Priority One or Two faults in order for the PSAP/ECC cutover(s) to occur.			
2. The selected Respondent shall provide a baseline Call-Handling Acceptance Test Plan (including specific test cases, scenarios, and expected outcomes) to INCOG at least 30 days in advance of the planned execution thereof and allow INCOG a full two weeks to modify the test plan to meet their system acceptance criteria.			
3. If a failure occurs, INCOG will provide a written notification to the Respondent with its classification of the fault according to the following four categories: a. **Priority One** Fault — A critical system fault that renders the solution even partially inoperable. These faults are unacceptable to INCOG. b. **Priority Two** Fault — A major system fault that significantly reduces the solution's performance and ability to function. These faults are unacceptable to INCOG and must be resolved before INCOG will accept the solution. c. **Priority Three** Fault — A minor system fault that marginally affects system performance and functionality. These minor faults are operational in nature and are only acceptable during the acceptance phases. These faults must be resolved before INCOG will accept the final solution. d. **Priority Four** Fault — A combination of minor system faults and items that are on a punch list or product roadmap. These are items that have minimal or no effect on system performance but must be resolved.			
4. If the Respondent disputes INCOG's fault classification, a call will be held at the earliest possible opportunity to resolve the disagreement. Parties to that call shall include INCOG, the Respondent, and, at INCOG's discretion, representative(s) from the PSAP/ECC. If agreement is not reached within 30 minutes, INCOG's classification will prevail.			
5. The Respondent shall remedy the non-compliance per the Service Levels and Service Management Performance Standard sections of the contract and shall provide written notification of the remedy to INCOG.			

Requirements:	Complies	Does Not Comply	Partially Complies
6. The acceptance testing process shall continue until all test cases are executed without Priority One and Priority Two faults, meaning the PSAP/ECC cutover(s) are ready to commence.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.46 Call-Handling System Acceptance Testing

Requirements:	Complies	Does Not Comply	Partially Complies
1. INCOG's call-handling system acceptance testing is intended to validate overall system performance, especially system-level functionality not otherwise verifiable during individual PSAP/ECC acceptance testing and includes (but will not be limited to) testing of areas such as the following: a. Inter-PSAP/ECC transfers and conferences. b. Automatic system failover and maintenance of full system functionality when a redundant element is taken out of service. c. Alternate routing under functional element and network component failure scenarios. d. High call volume performance.			
2. Call-handling system acceptance testing cannot begin until INCOG has successfully completed PSAP/ECC call-handling acceptance testing. The testing period shall be sufficient to demonstrate the solution's			

Requirements:	Complies	Does Not Comply	Partially Complies
performance and reliability. The period shall be 30-consecutive calendar days with zero Priority One and zero Priority Two faults.			
3. The selected Respondent shall provide a baseline System Acceptance Test Plan (including specific test cases, scenarios, and expected outcomes) to INCOG at least 30 days in advance of the planned execution thereof and allow the contracting PSAP/ECC(s) a full two weeks to modify the test plan to reflect their system acceptance			
4. If a failure occurs: a. INCOG will provide a written notification to the Respondent with its classification of the fault according to the four categories identified in Section 4.44 of this document.			
b. If the Respondent disputes INCOG's fault classification, a call will be held at the earliest possible opportunity to resolve the disagreement. Parties to that call shall include INCOG, the Respondent, and, at INCOG's discretion, representative(s) from the PSAP/ECC. If agreement is not reached within 30 minutes, INCOG's classification will prevail.			
c. The Respondent shall remedy the non-compliance per the Service Levels and Service Management Performance Standard sections of the contract and shall provide written notification of the remedy to INCOG.			
d. The acceptance testing process shall continue until all test cases are executed without Priority One and Priority Two faults, meaning the PSAP/ECC cutover(s) are ready to commence.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.47 Transition Plan

Requirements:	Complies	Does Not Comply	Partially Complies
1. Within 30 days of contract signing, the selected Respondent shall provide a detailed transition plan that shall include a full description of the methods and procedures that will be employed to ensure a non-service-affecting transition from the current call-handling environment to the new system.			
2. The selected Respondent shall provide recommendations considering the complexity of the specific deployment environment.			
3. The transition plan may include a suggested order for agency migration and provide projected time durations to complete the specific site, based on position count and other information the Respondent has learned regarding INCOG's configuration.			
4. The migration plan shall include a fallback procedure to restore the PSAP/ECC to a pre-transition operational state in the event of a severe failure.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.48 Product Lifecycle Management (PLM)

4.48.1 Software Release Management

Requirements:	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 all INCOG PSAPs/ECCs at no cost while a maintenance agreement is in place.			
3. The Respondent shall describe the frequency of defect-resolution software releases, and the decision-making processes involved in selecting which software defects to fix.			
4. The Respondent shall notify and coordinate scheduling with INCOG whenever solution servicing requires onsite visits. Notification shall occur no less than ten business days before the needed visit and scheduling shall be at the sole discretion of INCOG.			
5. The Respondent shall include in its proposal the procedure to manage and track system changes. This is especially important when changes affect the performance 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 INCOG staff.			
6. The Respondent shall provide release notes to INCOG no less than ten business days prior to system upgrades or updates, clearly identifying any new functionality of which INCOG may wish to take advantage.			
7. The Respondent shall request authorization from INCOG no less than ten days prior to performing maintenance, upgrades, backups, restorations, or other system changes that may impact the performance or functionality of the system or service (depending on how the call-handling solution is procured). The only exception to this advance-notice requirement is in cases where an update or upgrade is immediately required to restore a failed or failing service or component.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.48.2 Warranty and Monitoring

Requirements:	Complies	Does Not Comply	Partially Complies
1. For all software and Respondent-provided hardware, the Respondent shall include 24 x 7 x 365 parts and labor warranty for the duration of the contract (ten years) from the date of final INCOG acceptance. The Respondent shall provide 24 x 7 x 365 extended warranty (parts and labor) for optional two-year extensions.			
2. For all software and Respondent-provided hardware, warranties shall cover hardware, cabling and connectors, and software, and include 24 x 7 x 365 phone/web support.			
3. The Respondent shall include 24 x 7 x 365 remote system monitoring and maintenance. The Respondent shall describe its monitoring facilities (NOC/SOC, primary, secondary, backup, etc.), the level to which monitoring is performed (e.g., workstation, router in back room, etc.), and staffing to both monitor and respond.			
4. The Respondent shall describe NOC services, including proactive and reactive maintenance plans. The response shall include details regarding the number of certified technicians who will reside within a two-hour drive time to each call-handling site.			
5. System monitoring shall include a near-real-time portal through which the PSAP/ECC may configure a dashboard-type view for monitoring its data and voice activity as well as overall system status and health.			
6. The Respondent shall describe how out-of-warranty items are repaired or replaced. The Respondent shall describe the processes and procedures along with the estimated cost for all system components.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.49 Incident and Trouble Reporting

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall describe the procedures involved for initiating, tracking, communicating status, and resolving trouble reports. The Respondent shall describe all capabilities available with the solution, including remote monitoring, maintenance, troubleshooting, and repair.			
2. In addition to the built-in capabilities, the Respondent shall describe capabilities to interface with other management systems using standard protocols such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (CMIP).			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.50 Escalation Procedures

Requirements:	Complies	Does Not Comply	Partially Complies
1. Following cutover, INCOG may require escalation of an issue for resolution. The Respondent shall provide: a. Documentation of the escalation process along with names, titles, and contact information. b. The after-hours escalation process, if it is different from normal work hours. c. The process for updating escalation documentation as personnel changes occur during the contract period.			
2. The Respondent shall identify the specific issues, address how future occurrences will be avoided (risk mitigation), and provide a suggested path toward resolution.			
3. The escalation process shall address inclusion of the manufacturer (if other than Respondent) in meetings and discussions with affected PSAPs/ECCs when the Respondent's efforts have not resolved the issue.			
4. Escalation processes shall describe in detail the procedures for INCOG regarding resolution of critical defects, including time to resolution and engagement of Tier 3 or Tier 4 engineering and development resources.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.51 Software Backup and Restoration

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall perform automatic backups of software, as well as all PSAP/ECC-specific configurations and databases. The backups cannot affect system performance.			
2. The Respondent shall describe in detail, in the proposal, the recommended backup schedule on the workstations, servers, and any other customer-premise-installed devices that have databases, operating systems, and/or configurations that may be backed up.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.52 Maintenance and Repair History Log

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide, utilize, and maintain an online history log for all INCOG sites that tracks all system issues, resolutions, configuration changes, upgrades, etc. that are performed onsite or remotely. The Respondent shall describe the process for managing the history log and provide read access to INCOG.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.53 Spares and Advance Replacement

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall include a critical spares kit for all customer-premise-installed equipment. Any spares used out of the kit shall be replaced within 24 hours with tracking information about the shipment provided in advance.			
2. The Respondent shall describe the plan for maintaining a readily available cache of replacement parts to be available for delivery onsite within the response time frames outlined in *Appendix A.1 – Performance Standards and Terms*.			
3. The Respondent shall provide pricing and documentation describing the repair and advance-replacement processes for out-of-warranty solution components purchased (versus leased) by INCOG.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.54 CHE Documentation

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall provide documentation for all user-accessible configurations.			
2. The Respondent shall provide CHE technician certification training for interested INCOG staff.			
3. The Respondent shall provide documentation for an MIS solution, if provided, including: a. Sample reports. b. Report customization and automation; and c. Ad hoc report design, including best practices.			
4. The Respondent shall provide administrator guide(s) including screen layout customization and speed-dial directory maintenance, import, and export, user account management, etc.			
5. The Respondent shall provide telecommunicator quick reference cards for call handling, mapping, discrepancy reporting, and other provided systems.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.55 Artificial Intelligence and Machine Learning

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall describe the artificial intelligence (AI)/machine learning (ML) capabilities of the proposed CHE system.			
2. The Respondent shall describe their ability to apply AI/ML technology to answer administrative (non-911) calls.			
3. The Respondent shall describe opportunities to apply AI/ML technologies and techniques to the analysis of multimedia content delivered to the PSAP/ECC.			
4. The Respondent shall describe their ability to apply AI/ML technology to excessive calls coming from the same location.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

4.56 CHE Performance Standards and Service Level Requirements

Requirements:	Complies	Does Not Comply	Partially Complies
1. The Respondent shall describe how the proposed solution(s) will meet the requirements and definitions in *Appendix A.1 – Performance Standards and Terms* of this solicitation package.			
2. The Respondent shall describe how the proposed solution(s) will meet the requirements in *Appendix A.2 – IP Network Measurement and Reporting Requirements* of this solicitation package.			

Requirements:	Complies	Does Not Comply	Partially Complies
3. The Respondent shall describe how the proposed solution(s) will meet the requirements in *Appendix A.3 – Service Level Agreement* of this solicitation package.			

Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Add additional lines as needed.

Appendix, Attachment, and Exhibit Guide

Table 2: Exhibit Guide

Section	Title	Page
Appendix A	CHE Performance Standards, Network Measurement and Reporting, and Service Level Agreements	
Attachment A	Pricing Matrix	

Appendix A: Performance Standards, Network Measurement and Reporting, and Service Level Agreements

1. **Performance Standards and Terms**

A. Service Level Agreement

An agreement between INCOG and the Respondent that specifies, in measurable terms, the services that the Respondent will furnish.

B. Help Desk Availability

The time of day resources are available to answer calls from INCOG, create trouble tickets and dispatch technicians.

Resources must be available (via tollfree telephone number) 24 x 7 x 365 to process requests for service.

C. Technician Availability

Technicians must be available remotely and/or onsite as required, 24 x 7 x 365.

D. Regular Business Hours (RBH)

Hours between 8:00 a.m. and 5:00 p.m. Eastern.

E. 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.

F. System Availability

The service must be available at least 99.999 % of the time, measured on a per-PSAP/ECC basis.

G. 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.

H. Web-Based Trouble Reporting and Tracking

It is desirable that trouble reporting and escalation tracking are reported via a secure web-based portal.

I. Fault Priority Levels

Fault priority level definitions are the same as those in Acceptance Testing. For the post-cutover environment, some examples are provided below of issues which would be considered of the specified priority.

1) Priority One – Critical

A fault shall be categorized as “Priority One” if it is characterized by the following attributes: the fault (a) renders a business critical system, service, software, equipment or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects a single individual or a group of people performing a critical business function. Examples of these conditions may 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.
- Software defect without a workaround that impacts any site or site’s ability to maintain business operations.
- A reduction in call processing capacity at a single site of 50% or more.

2) Priority Two – Major

A fault shall be categorized as a “Priority Two” if it is characterized by the following attributes: the fault (a) does not render a business-critical system, service, software, equipment or network component 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 (b) affects a single individual or group of people performing a critical business function. Examples of these conditions may include:

- Loss of network or redundancy, including a CHE node or PSAP connectivity.
- System or component problem that could result in loss of a site without timely repair.
- A reduction in call processing capacity at a single site of 20% or more.
- Inability to accurately display critical information like caller telephone number or location.

3) Priority Three – Minor

A fault shall be categorized as a “Priority Three” if it is characterized by the following attributes: the fault causes a group or individual to experience trouble accessing or using a system, service, software, equipment or network component, or a key feature thereof, and a reasonable workaround is not available, but does not prohibit the execution of productive work. Examples of these conditions may include:

- Inability for certain users or roles from performing their job function.

- Failure of a semi-common function like call monitoring, or custom greetings, or a small display problem, requiring manual intervention or other additional steps to achieve the desired result.

4) Priority Four – Non-service-impacting

A fault shall be categorized as a "Priority Four" if it is characterized by the following attributes: the fault impacts a group or individual affected by planned maintenance of the "service" or non-service impacting incident. Examples of these conditions may include:

- Errors in data display/presentation within a user's application (layout, colors, data identification, etc.)
- Errors with peripheral systems such as recorders, MIS, auxiliary keypads, etc.
- Errors with monitoring systems, dashboards, etc.
- Items committed to by the Respondent that are planned for a future release (software development)

J. Response or Notification Time

The time elapsed between identification of an issue (by monitoring staff or by INCOG) and commencement of investigation or repair activity by the Respondent.

Table 3: Maximum Response Time

Fault Priority	Response Time
Priority One	15 minutes
Priority Two	30 minutes
Priority Three	8 hours
Priority Four	Next Business Day

K. Repair Time

The time elapsed between identification (by monitoring staff or by INCOG), and the resolution of that issue, with full functionality and capacity restored to normal. At the discretion of the reporting party(ies), "resolution of that issue" may be achieved by the deployment of a workaround, if accompanied by a mutually agreeable written plan for definitively resolving the original issue.

Table 4: Maximum Repair Time

Incident Severity	Maximum Repair Time
Priority One	2 hours
Priority Two	4 hours
Priority Three	48 hours
Priority Four	5 business days

L. Escalation

A request for assistance to the next higher level of technical support must be executed whenever the *Escalation Interval* (in the following table) has elapsed since the issue was identified or reported and issue remains unresolved. Once an escalation has occurred, the Respondent will provide INCOG and affected parties with a status update at the *Update Interval* until the issue has been resolved.

Table 5: Expected Escalation Intervals

Incident Severity	Escalation Interval	Update Interval
Priority One	1 hour	2 hours
Priority Two	4 hours	8 hours
Priority Three	48 hours	24 hours
Priority Four	96 hours	As agreed to

2. **IP Network Measurement and Reporting Requirements**

A. 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. The CHE network refers to both node-to-node and node-to-PSAP connections.

B. Outage Reporting

In the event of an unplanned outage, the Contractor must provide to INCOG a Reason for Outage (RFO) report. This report will include a timeline of the outage, the cause of the outage, actions taken to resolve the issue, and any actions/processes undertaken by the Respondent and its subcontractors to prevent similar outages from occurring in the future or to mitigate their impact, if they do. INCOG requires a preliminary report within five business days and a final report within 30 calendar days to be measured from detection of the outage.

As defined in 47 CFR § 4.5, the Respondent is responsible for complying with all federal reporting requirements for any outages or interruptions to 9-1-1 voice or SMS text, delivery, and/or processing systems and services provided under a contract. The Respondent is required to electronically report significant network outages and information about outages that exceed specific thresholds—in terms of duration and magnitude—to the FCC's Network Outage Reporting System (NORS). The electronic report shall also include information regarding communications disruptions affecting any 9-1-1 facilities.

C. Bandwidth Management

The Respondent shall provide monthly bandwidth performance and network utilization reports.

INCOG must be able to monitor overall bandwidth usage and specific usage between sites. INCOG must be able to view real-time or near-real-time bandwidth performance and utilization reports. Users of the monitoring tools should be able to filter on various traffic characteristics (e.g., protocol, QoS classification, media type, etc.). A web-based portal or browser-enabled viewer is preferred.

The Respondent's call-processing capacity shall be capable of 125% busy hour call traffic for the PSAP/ECC.

The Respondent's service shall be able to increase call-processing capability by up to 50% over contract duration with no critical hardware upgrades required.

D. Voice Quality and Quality of Service

Voice quality must be maintained at traditional Public Switched Telephone Network (PSTN) levels. Voice data (RTP[6]) must have priority over any other IP traffic and this priority must be respected and enforced by all network infrastructure elements, end-to-end. The service shall use an uncompressed, high quality voice codec. The CHE must not degrade the Mean Opinion Score (MOS) of calls traversing its network by more than two-tenths (0.2) and must maintain a Mean Opinion Score (MOS) standard rating of 4.0 or higher.

E. Network Management and Monitoring

The Respondent must provide a NOC to respond to network issues and meet the service levels stated within this document, including requirements for a secondary or backup NOC.

---

[6] *Real-time Transport Protocol*

F. Proactive Monitoring

The Respondent must provide active monitoring of its Service as a whole, including; network, replication, hardware, software, call processing, etc. The Respondent must proactively generate incident tickets and alert INCOG and affected PSAPs/ECCs in accordance with the fault priority tables above regarding Response or Notification Times.

3. Service Level Agreement

Respondents shall provide a description of their SLA reporting tool and shall provide a point of contact for any identified incidents or service failures. A secure online SLA reporting dashboard is preferred. SLA reporting tools are expected to include both real-time and near-real-time performance statistics calculated at no greater than 5-minute intervals. 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 INCOG monthly. 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 web-based portal is preferred. Other relevant data also may be reported.

Respondents shall specify how they 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.

Service Level Requirements (SLR) remedies shall be tracked to their full amount, but the maximum credit per month shall not exceed 25% of the total amount at risk (as defined, below).

Incidents shall be tracked via tickets and the ticket contents shall be made available to INCOG and the affected PSAP/ECC(s) via an online portal with the ability to download or print reports.

The Respondent shall have automated systems to track all SLA deliverables and provide INCOG with monthly reports detailing the Respondent's performance.

The monthly SLA compliance report shall include the following detail and a one page summary of the detail:

1) Report period
2) Contractor's trouble ticket number
3) Name(s) of affected PSAP/ECC(s)
4) FCC ID(s) of affected PSAP/ECC(s)
5) Service type
6) Brief trouble symptom
7) Brief restoration description
8) Trouble symptom category
9) Ticket open date and time
10) Priority level
11) Problem resolution date and time
12) Total outage duration
13) Yes/no if qualified for SLR remedy
14) Yes/no if FCC reporting required; and
    a. If Yes, link to FCC report and FCC response, if any

15) Applicable SLA

The following table details INCOG's SLRs, providing a description of each, the metric or measurement to be used to confirm compliance, the target measurement, and the affected party or parties' (INCOG or PSAP/ECC[s]) rights and remedies, in the event that the Respondent fails to achieve the SLR.

For SLR violations, the remedy listed in the table, below, may be a portion of "the amount at risk". For the purposes of this section, "amount at risk" is defined, as follows:

- For services or solutions incurring a monthly recurring charge (MRC), "amount at risk" shall be the MRC for that service or solution for the month in which the SLR violation occurs.
- For services or solutions including a non-recurring charge (NRC) component, "amount at risk" shall be the total NRC for that service or solution for the duration of the contract divided by the number of months in the contract – in other words, one month's portion of the NRC for that service or solution.
- For services or solutions including both NRC and MRC, "amount at risk" shall be the total of the two amounts described above.

Table 6: Service Level Requirements, Metrics, and Remedies

#	Definition	Measurement Method	Objective	Rights and Remedies
1	Final master project plan (MPP) shall be delivered to INCOG 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 INCOG 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).

#	Definition	Measurement Method	Objective	Rights and Remedies
3	SLA Remedy Delivery – Timely credit or adjustment of remedies due to INCOG for missed SLR objectives.	Calendar Days	Contractor's credit or adjustment shall be issued no more than 60 calendar days after written notice from INCOG 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	Contractor shall report all outages that potentially impact the delivery of 911 traffic to every affected PSAP and INCOG within 15 minutes of the occurrence.	Any outage that potentially impacts the delivery of 911 traffic, regardless of traffic type.	Notification of PSAPs and INCOG 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.

#	Definition	Measurement Method	Objective	Rights and Remedies
6	Failure to provide updates to solution to conform to NENA i3 standards within 18 months of ratification.	Identification by INCOG 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 and/or call handling, as applicable, until conformance issue is resolved to INCOG's or a PSAP's/ ECC's satisfaction.
7	CHE must handle voice calls with little or no degradation of voice quality of the call from the ESInet demarcation point to the workstation, as measured and monitored by an automated MOS measurement tool at the endpoint.	Ingress demarcation point shall be defined as the handoff point to the call handling equipment hosts. Egress demarcation point shall be the call-handling workstation.	Egress MOS measurements shall be maintained at 4.0 or better.	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/ECCs 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/ECCs 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/ECCs that month.
8	CHE will receive and handle all call type traffic with minimal service interruption.	Single outage with a duration of six minutes or more.	Preventing CHE outages of six minutes or more.	100% credit or adjustment of the amount at risk for call handling for the affected PSAPECC(s).
9	CHE will receive and handle all call type traffic with minimal service interruption.	Single outage of greater than two minutes and less than six minutes.	Preventing CHE outages greater than two minutes, but less than six minutes.	50% credit or adjustment of the amount at risk for call handling for the affected PSAP/ECC(s).

#	Definition	Measurement Method	Objective	Rights and Remedies
10	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 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.
11	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 INCOG and the impacted PSAP/ECC(s) 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.
12	Contractor shall provide a Reason for Outage (RFO) report for Priority One and Two issues within five business days.	Business Days	Contractor shall deliver initial RFO report to INCOG and the affected PSAPs/ECCs within five 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.
13	Contractor shall provide a final root cause analysis report within 30 calendar days from the beginning of the service affecting issue.	Calendar Days	Contractor shall deliver final root cause analysis to INCOG and the affected PSAPs/ECCs within 30 calendar 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.