TXShare

Your Public Sector Solutions Center

# REQUEST FOR PROPOSALS
# For
# Standards-Based NG9-1-1 Functional Elements Supporting CHE, Data Analytics, Dispatch Mapping, and Ancillary Services

## 2026-033

March 2026

TXShare
Your Public Sector Solutions Center

**REQUEST FOR PROPOSALS**
**For**
**Standards-Based NG9-1-1 Call Handling System Including Required Functional Elements**
**RFP # 2026-033**

Sealed proposals will be accepted until 2:00 PM CT, **April 17, 2026,** and then publicly opened and read aloud thereafter.

_____
Legal Name of Proposing Firm

_____
Contact Person for This Proposal Title

_____
Contact Person Telephone Number Contact Person E-Mail Address

_____
Street Address of Principal Place of Business City/State Zip

_____
Mailing Address of Principal Place of Business City/State Zip

_____
Point of Contact for Contract Negotiations Title

_____
Point of Contact Telephone Number Point of Contact Person E-Mail Address

Is your business currently registered with the Texas Secretary of State to transact business in Texas?
☐ Yes ☐ No

Texas Secretary of State Filing Number (if applicable): _____

Acknowledgment of Addenda (initial): #1_____ #2 _____ #3 _____ #4 _____ #5 _____

**NOTE: Any confidential/proprietary information must be clearly labeled as "confidential/proprietary". All proposals are subject to the Texas Public Information Act.**

# TABLE OF CONTENTS

## SECTION 1: OVERVIEW

### 1.0 PURPOSE

The North Central Texas Council of Governments ("NCTCOG") seeks an experienced vendor or vendors to provide a **standards-based Next Generation 9-1-1 (NG9-1-1) Call Handling System, including required functional elements**, as described herein, to the members of its TXShare Cooperative Purchasing Program ("TXShare"). The awarded contract(s) will be promoted through TXShare.

The purpose of this Request for Proposals (RFP) is to solicit responses that result in a contract with one or more vendors that are qualified to provide one or more categories of NG9-1-1 call handling solutions and related functional elements in accordance with nationally recognized standards.

The desired service categories are listed below:

**Service Category #1: Standards-Based NG9-1-1 Call Handling System (CHE)**

**Service Category #2: Dispatch Mapping Solution for NG9-1-1**

**Service Category #3: Data Analytics Solution for NG9-1-1**

**Service Category #4 Ancillary Services for NG9-1-1**

1.0.1 Definitions:

- **Contractor** – An Offeror that has been awarded a contract under this RFP.
- **Customer** – A governmental entity.
- **Governmental Entity** – A government agency or non-profit organization.
- **RFP** or **Solicitation** – This Request for Proposals document.
- **Vendor** – A business interested in providing goods or services under this RFP.
- **Offeror, Respondent** or **You** – A Vendor that submits a proposal in response to this RFP.

1.0.2 Outcome

The desired outcome of this RFP is for NCTCOG to enter into a Master Services Agreement ("MSA") with one or more Contractors to supply municipalities, counties, school districts and other governmental agencies ("Customer," "Government Entity") with assistance to obtain the described services from fully licensed vendors authorized to do business in the locations selected in Exhibit 3.

NCTCOG intends to award Contracts through its TXShare purchasing cooperative to multiple Contractors. Members of TXShare ("Customer" or "Member") will have the option to utilize these contracts to fulfill their needs. The contract award does not guarantee any specific number of sales to any firm awarded this contract. The goods or services will be provided on an as-needed basis. There are no scheduled orders at this time, but there is the expectation that needs will arise among various Customers of the TXShare cooperative. Vendors awarded contracts will be uniquely positioned to market their products to the Customers. Each Customer will negotiate their own orders on an as-needed basis.

## SECTION 2: TXSHARE COOPERATIVE PURCHASING PROGRAM

### 2.0 BENEFITS OF A COOPERATIVE PURCHASING PROGRAM

2.0.1 How Does a Cooperative Purchasing Program Work?

A government cooperative purchasing program, such as TXShare, is a cooperative arrangement for acquiring goods or services that involves aggregating the demand of two or more government agencies to obtain a more economical purchase.

Government entities (cities, counties, water districts, school districts, etc.) sign up as members to use cooperative purchasing programs through a cooperative purchasing agreement. Additionally, non-profit organizations are allowed to sign up as members.

2.0.2 How Does a Government Entity Benefit?

Cooperatives help government agencies find the right goods and services that best fits their needs and expedite purchases without requiring additional solicitations (RFP or IFB) to comply with laws and regulations.

TXShare uses the North Central Texas Council of Governments ("NCTCOG") as the lead public entity to publicly solicit and award contracts through a Request for Proposal ("RFP") process. TXShare members are eligible to access these contracts by signing an intergovernmental agreement with NCTCOG, thereby eliminating the need to complete their own RFP process.

Membership in the TXShare cooperative purchasing program provides the agencies with access to contracts for goods and services at pre-negotiated rates or prices. Typically, the entity member then purchases the goods or services by negotiating with the cooperative's awarded vendors and places purchase orders, or enters into sub-agreements, based on the rates or prices listed in the cooperative purchasing program's contracts.

2.0.3 How Does A Vendor Benefit?

A Request for Proposal (RFP) such as this one is a document that competitively solicits bids from potential vendors for goods or services. The lead public entity (NCTCOG) is an independent government entity that carries out the advertising and bid procedures required by state law.

All of TXShare's contracts are competitively bid and publicly awarded through this process. NCTCOG prepares the RFP incorporating the required cooperative purchasing language that allows its entity members across the nation to utilize the awarded contract(s).

Vendors respond to the RFP by submitting their proposals. NCTCOG evaluates the responses and awards a Master Services Agreement for the TXShare cooperative, thus establishing the availability for nationwide use of the resulting contracts.

Vendors who successfully compete in the RFP process and are awarded a contract will market to any public entity or nonprofit and can then forgo the RFP process for an individual entity.

When marketing to a customer, the awarded vendor can provide a quote to the customer for its unique needs based on the pricing, terms and conditions of its contracts. For a vendor, being awarded a cooperative contract can help shorten the sales cycles considerably. This is especially beneficial for smaller firms, like startups, that may not otherwise be able to access the government market.

2.0.4 Mutual Benefits

Performing a competitive bidding process typically takes in excess of 90 days to create the RFP solicitation, collect and evaluate proposals, then negotiate and award the contract. Reducing the amount of time that purchasing staff spend managing new solicitations and generating new contracts, especially for goods or services that don't require too much customization, saves months

of administrative time and effort. Reducing the need to respond to every bid process and market directly to the customer saves time and money as well as is an "ace in the hole" for a vendor when closing the sale on its goods or services covered by a cooperative contract. Smaller governments' customers can achieve price-saving advantages from purchasing off a cooperative program with greater purchasing power.

Note: There is no obligation on the part of any Customer to purchase goods or services through the awarded contracts nor is there any guarantee, implied or otherwise, that the awarded contractor(s) will make any sales based on this solicitation.

## 2.1 NCTCOG OVERVIEW

NCTCOG is a voluntary association of, by, and for local governments and was established to assist local governments in planning for common needs, cooperating for mutual benefit and coordinating for sound regional development. NCTCOG serves a 16-entity metropolitan region surrounding the cities of Dallas and Fort Worth.

NCTCOG's governing structure is as follows: each member government appoints a voting representative from their governing body. These voting representatives comprise the General Assembly, which annually elects a 17-member Executive Board. The Board also includes one ex-officio non-voting member of the legislature. The Executive Board is supported by policy development, technical advisory, and study committees, as well as professional staff.

## 2.2 TXSHARE OVERVIEW

TXShare is a cooperative purchasing program administered by NCTCOG. The program is designed to streamline procurement for public entities by offering competitively solicited contracts that meet state, local, and federal purchasing requirements. Currently the TXShare Purchasing Cooperative has over 300 members from across the USA, including counties, cities, school districts, and special districts.

## 2.3 PROGRAM EXPLANATION

NCTCOG intends to make the contract awarded from this solicitation available to other public entities through TXShare. By promoting their TXShare contract(s) to public entities, contractors reduce the need to repeatedly respond to public customer bids or RFPs. The contractor then realizes substantial efficiencies that will increase sales opportunities. Contractors agree to pay an administrative fee to TXShare, calculated as a percentage of sales processed through the TXShare contracts awarded and held by the contractor. This administrative fee is not an added cost to be invoiced by the contractor to TXShare participants. This administrative fee covers the costs of contract marketing and facilitation incurred by TXShare.

Under the TXShare program, any public customer or nonprofit can use the TXShare contract and its selected contractor(s) to make purchases necessary to pursue their own needs. Offerors awarded a contract under the TXShare program may offer their services nationwide if they desire to do so. The TXShare contract offers a unique advertising advantage to a contractor to promote its services, as the contract satisfies most public entities' procurement requirements.

## 2.4 CONTRACT MANAGEMENT AND REPORTING

The contractor will be required to track and report to NCTCOG its TXShare sales activities relating to the master contract. The contractor will be required to provide management reports on a quarterly basis. Examples of management report data include, but are not limited to:

- Participating public customer's name; pricing option chosen; total fee charged. NCTCOG and contractor will agree to form and content of reports after award of contract.

## 2.5 ADMINISTRATIVE FEE

TXShare will collect an administrative fee, in the form of a percentage of sales, that will apply to all sales between the contractor and public entities using the cooperative program awarded contract. NCTCOG is included as a public entity customer as it may also make purchases through the contract. The administrative

fee will be remitted by the contractor to NCTCOG on a quarterly basis, along with required quarterly reporting. The administration fee for this program will be 2.5% of sales.

## 2.6 INTERLOCAL AGREEMENT

Governmental entities are extended the opportunity to purchase from contracts awarded by NCTCOG TXShare purchasing cooperative by virtue of an interlocal agreement between the entity and NCTCOG. However, all parties understand, and all parties hereby expressly agree, that NCTCOG is not an agent of, partner to or representative of those government entities and that NCTCOG is not obligated or liable for any action or debts that arise out of the government customer's purchase.

## 2.7 STANDARD TERMS AND CONDITIONS

NCTCOG Procurement Standard Terms and Conditions can be found at www.nctcog.org in the "Open Solicitations" section, or by clicking here. Proposers shall certify its compliance with these requirements as part of their proposal response by completing the certifications included with the RFP document "Attachments" section. Failure to submit the required certification statement may be grounds for finding the proposal nonresponsive.

## 2.8 RESPONDENT ELIGIBILITY

Firms that are legally required to register with the Texas Secretary of State must provide their current filing number on the Cover Page (page 2 of this solicitation document). Proposals submitted by entities that are required to register and maintain an active status to transact business in Texas, but do not include a valid filing number or are not in good standing at the time of submission, may be considered non-responsive and may not be evaluated further.

## SECTION 3: GENERAL INFORMATION

### 3.0 CONTRACT INTENT

NCTCOG intends to contract with one or more qualified Offeror(s) based upon the qualifications of the Offeror and the categories of goods or services they are able to provide. However, NCTCOG anticipates exploring any viable alternative for providing these goods or services and may decide, after reviewing the proposals submitted, to reject all proposals and not to enter into any agreement.

### 3.1 ADMINISTRATIVE GUIDANCE

The information provided herein is intended to assist vendors in the preparation of proposals necessary to properly respond to this solicitation. The solicitation is designed to provide interested vendors with sufficient basic information to submit proposals meeting minimum requirements but is not intended to limit a submission's content or to exclude any relevant or essential data there from. You are at liberty and are encouraged to expand upon the specifications to give additional evidence of your ability to provide the services requested in this solicitation.

### 3.2 ADDENDA

Addenda to this solicitation will be made available to vendors of record by posting the addenda on the BidNet Direct website. A "vendor of record" is defined as a vendor who has downloaded the solicitation directly from the BidNet Direct website. It is the vendor's responsibility to check for any addenda that may be issued. You shall acknowledge receipt of addenda by checking the appropriate spaces on the cover sheet of this RFP and submit with their proposal.

### 3.3 SOLICITATION SCHEDULE

The anticipated schedule for the RFP process is given below. All times indicated are Central Time (CT).

The anticipated schedule is as follows:

| | | |
|---|---|---|
| **RFP Issued** | **March 9, 2026** | |
| **Pre-Proposal Conference** | **March 16, 2026** | **10:00 AM CT** |
| **Inquiry Period Ends** | **March 31, 2026** | **5:00 PM CT** |
| **Proposal Due Date** | **April 17, 2026** | **2:00 PM CT** |
| **Planned Contract Award** | **May 2026** | |

NCTCOG reserves the right to change this schedule at any time.

### 3.4 PRE-PROPOSAL CONFERENCE

There will be a non-mandatory pre-proposal conference at 10:00 AM on **March 16, 2026,** via Microsoft Teams. The invitation is as follows:

**Microsoft Teams meeting**
**Join: https://teams.microsoft.com/meet/23860878452584?p=yezUaiEj4TXyUECdAv**
**Meeting ID: 238 608 784 525 84**
**Passcode: NB9MR6DR**

---

**Need help? | System reference**
**Dial in by phone**
**+1 903-508-4574,851572682# United States, Tyler**
**Find a local number**
**Phone conference ID: 851 572 682#**

## 3.5 QUESTIONS AND REQUESTS FOR CLARIFICATION (INQUIRY)

Vendors will have the ability to submit questions in writing via the BidNet Direct by Sovra ("BidNet Direct") platform until the proposal deadline. However, it is important to note that questions received less than seven (7) days prior to the proposal due date may not be answered in a timely manner. Vendor-specific questions about the process will often be answered directly. However, substantive questions that are not properly addressed in the solicitation information will be properly published to all vendors as an addendum or "Question & Answer" document. Proposers are responsible for reviewing the BidNet Direct website for any updates related to this RFP prior to the closing date.

## 3.6 PROPOSAL SUBMISSION

NCTCOG utilizes BidNet Direct by Sovra ("BidNet Direct") as the central eProcurement portal for all formal procurement opportunities. In order to respond to this RFP, as well as receive notifications, updates, addenda, and other information regarding this solicitation, NCTCOG requires that Respondents be registered with BidNet Direct.

Registration with BidNet Direct is free and allows Offerors to view all of NCTCOG's active procurement solicitations. The landing page for this project is found here.

Electronic submission of proposals shall be made in English, in searchable PDF format, and must be uploaded via BidNet Direct no later than **2:00 PM (Central Time) on April 17, 2026.**

It is the responsibility of Respondents to ensure that proposals are received at the NCTCOG address as described above by the designated due date and time. NCTCOG assumes no responsibility for delays caused by postage, mail courier, email, package misdirection or any other form of delivery. Late proposals will be not be opened nor considered in the evaluation of the proposal. Proposals may be withdrawn at any time prior to the submittal deadline, but they may not be withdrawn after the official opening.

**Submission Support and Guidance:**
For assistance with the submission process, please refer to this helpful video: **Creating and Submitting a Bid**.

It is **strongly recommended** that proposals be submitted at least 12 to 24 hours prior to the deadline to allow sufficient time for BidNet Direct to address any technical issues that may arise with the platform.

For BidNet Direct Vendor Support, please contact:
- **Phone:** (800) 835-4603 (Option 2)
- **Email:** support@bidnet.com

Proposals received will be publicly opened after the response submission deadline on BidNet Direct. Only the names of the vendor submitting the proposal will be read aloud. No other information will be disclosed at that time.

Proposal information is restricted and not publicly available until after award of a contract. All documents associated with the proposal submitted, unless the respondent indicates a portion of the proposal is proprietary, may be subject to public inspection in accordance with the Public Information Act. All information obtained in the course of this solicitation will become property of NCTCOG.

**NOTE: Any confidential/proprietary information must be clearly labeled as "confidential/proprietary". All proposals are subject to the Texas Public Information Act.**

## 3.7 PUBLIC OPENING

The public opening for this RFP will be conducted beginning approximately 2:05 PM CT on the date proposal submissions are due. The opening meeting will be held virtually via Microsoft Teams and will be recorded. Please note that a large volume of proposals may result in a lengthy opening process. Meeting access information and the Teams meeting invite will be posted to BidNet Direct prior to the date of the public

opening. Only the names of the Offerors submitting a proposal will be read aloud. No other information will be disclosed at the time of opening.

Proposal information is restricted and not publicly available until after award of a contract. All documents associated with the proposal submitted, unless the Offeror indicates a portion of the proposal is proprietary, may be subject to public inspection in accordance with the Texas Public Information Act. Any part of the proposal that you desire to declare as confidential information must be noted as such where the information is found in the proposal. Claims of confidentiality are subject to the opinion of the Texas Office of the Attorney General, should NCTCOG receive an open records request. All information obtained during this solicitation will become property of NCTCOG.

The opening will be on Microsoft Teams as follows:

**Microsoft Teams meeting**
**Join:** https://teams.microsoft.com/meet/28091548973650?p=VQrCpbnlFmnWXOPyyV
Meeting ID: 280 915 489 736 50
Passcode: aG32S3pB

---

Need help? | System reference
**Dial in by phone**
+1 903-508-4574,,383338862# United States, Tyler
Find a local number
Phone conference ID: 383 338 862#

Only the names of the Offerors submitting a proposal will be read aloud. No other information will be disclosed at the time of opening.

Any part of the proposal that you desire to declare as confidential information must be noted as such where the information is found in the proposal. Claims of confidentiality are subject to the opinion of the Texas Office of the Attorney General, should NCTCOG receive an open records request.

## SECTION 4: EVALUATION AND AWARD

### 4.0 TIME FOR EVALUATION

Unless stated otherwise elsewhere in this Request for Proposals, all proposals of qualification submitted shall remain valid for a minimum of 90 calendar days after the due date to allow adequate time for evaluation and award.

### 4.1 EVALUATION PROCESS

All submissions in response to this solicitation will be evaluated in a manner consistent with NCTCOG and all applicable rules and policies.

A proposal review committee will be assembled to perform the evaluations. In the initial phase of the evaluation process, the evaluation committee will review all proposals that have been received before the solicitation due date. Nonresponsive submissions (those not conforming to the solicitation requirements) will be eliminated. Each respondent bears sole responsibility for the items included or not included in the response submitted by that respondent. NCTCOG reserves the right to disqualify any submission that includes significant deviations or exceptions to the terms, conditions, and/or specifications in this solicitation.

NCTCOG reserves the right to reject any and all submittals and to waive any informality in submittals received, deemed to be in the best interest of NCTCOG.

### 4.2 BAFO AND CLARIFICATION REQUESTS

Once proposals have been submitted, NCTCOG evaluates the proposals and determines which of those are determined to be reasonably qualified for award. Those so determined will be reviewed and scored. Clarification requests may be requested of firms where clarifying information is necessary to better understand meaning of any part of a bid submission. Best and final offers ("BAFO") for those reasonably qualified may be obtained by allowing the submission of a BAFO before the final decision is made to award a contract.

NCTCOG reserves the right to be the sole judge as to the overall acceptability of any submission or to judge the individual merits of specific provisions within competing offers.

### 4.3 ORAL PRESENTATIONS

NCTCOG reserves the right to require a presentation by the firm to supplement their written submission. These presentations will be scheduled, if required, after Proposals are received and prior to the award of the Contract.

### 4.4 AWARD OF THE CONTRACT

Upon completion of the evaluation process, NCTCOG may award the contracts to one or more respondent(s) whose submission is determined to be the most advantageous to NCTCOG.

## 4.5 PROPOSAL EVALUATION CRITERIA

The criteria to be used to evaluate submissions are as follows:

| Pass/Fail Criteria | Description | Percentage Points |
|---|---|---|
| ***References*** | Points will be awarded on a pass/fail basis for the clear inclusion of the required information regarding ***References***, as outlined in greater detail in **Section 6.0**. | Pass/Fail - 5% |
| **Weighted Scoring Criteria** | | **Weighted Maximum Percentage Points** |
| ***Project-Related Experience and Qualifications*** | Points will be awarded based on the clear inclusion and quality of response regarding the required information regarding ***Project-Related Experience and Qualifications***, as outlined in greater detail in **Section 6.0**. | 25% |
| ***Technical Proposal*** | Points will be awarded based on the clear inclusion and quality of response regarding the required details of the ***Technical Proposal***, as outlined in greater detail in **Section 6.0**. | 50% |
| | | |
| ***Proposal Pricing*** | Points will be awarded based on responses to ***Exhibit 1 - Pricing***, as outlined in greater detail in **Section 6.0**. | 20% |
| | ***TOTAL POSSIBLE PERCENTAGE POINTS*** | ***100%*** |

# SECTION 5: SPECIFICATIONS

## 5.1 Scope of Work

The North Central Texas Council of Governments (NCTCOG), through its TXShare Cooperative Purchasing Program ("TXShare"), seeks to establish Master Services Agreements (MSAs) with one or more qualified vendors to provide a standards-based Next Generation 9-1-1 (NG9-1-1) Call Handling System and associated NG9-1-1 functional components.

TXShare contracts are made available to governmental agencies, municipalities, and eligible non-profit entities throughout the United States, enabling members to access competitively procured, high-quality public safety technologies and services.

Under the resulting agreements, awarded vendors will support TXShare members on an as-needed basis. Member agencies will initiate engagements directly with awarded vendors through project agreements, purchase orders, or statements of work.

Solutions provided under the resulting contract shall comply with nationally recognized NG9-1-1 standards and the industry standards identified in this RFP, and be interoperable, secure, scalable, resilient, and capable of supporting mission-critical public safety operations.

This Scope of Work includes the provision, implementation, configuration, integration, testing, training, maintenance, and ongoing support for NG9-1-1 systems and related components.

Vendors may propose solutions for one or more of the following service categories:

1. **Standards-based NG9-1-1 Call Handling System (Call-Handling Equipment [CHE])**
    1. Core call processing; Next Generation Core Services (NGCS) interfaces; multimedia handling; system provisioning; resiliency and redundancy; cybersecurity controls; and compliance with applicable National Emergency Number Association (NENA) i3 functional and interface standards.

2. **Dispatch Mapping Solution for NG9-1-1**
    1. Real-time geospatial mapping integrated with NG9-1-1 call handling; geographic information system (GIS)-based visualization; location validation; and compatibility with regional and member-provided GIS datasets.

3. **Data Analytics Solution for NG9-1-1**
    1. System performance analytics; operational metrics and call quality analysis; trend reporting; real-time dashboards; and standardized state and national reporting outputs.

4. **Ancillary Services for NG9-1-1**

Proposed solutions shall be capable of supporting diverse operational environments ranging from small rural public safety answering points (PSAPs) to large metropolitan 9-1-1 centers.

Vendors shall demonstrate technical expertise in NG9-1-1 environments, successful implementation experience, the ability to provide ongoing support, and reliability consistent with the mission-critical expectations of public safety communications.

Regardless of the service category proposed (CHE, Dispatch Mapping, and/or Data Analytics), all proposed solutions shall comply with the applicable General Requirements set forth in Section 5.3. In addition, each proposed solution shall comply with the specific technical and functional requirements identified in its respective section(s) (5.4 – 5.6)

of this RFP. Compliance with Section 5.3 is mandatory and shall apply in conjunction with, and not in lieu of, the requirements applicable to the specific solution category proposed.

## 5.2 INDUSTRY STANDARDS

NCTCOG seeks a standards-based solution that complies with nationally recognized standards and requirements applicable to Internet Protocol (IP) network architecture, core services, security, and interface functionality.

All aspects of the Respondent's proposed system design, deployment, operation, integration, and security shall comply with the standards, requirements, and recommendations identified in the following documents and promulgated by the following Standards Development Organizations (SDOs):

- Alliance for Telecommunications Industry Solutions (ATIS)
- American Institute of Certified Public Accountants (AICPA)
- Association of Public-Safety Communications Officials (APCO) International
- Center for Internet Security (CIS)
- Independent Electrical Contractors (IEC)
- Institute of Electrical and Electronics Engineers (IEEE)
- Internet Engineering Task Force (IETF)
- International Organization for Standardization (ISO)
- National Emergency Number Association (NENA)
- National Institute of Standards and Technology (NIST)
- Open Web Application Security Project (OWASP)
- Telecommunications Industry Association (TIA)
- The Monitoring Association (TMA) (formerly known as the Central Station Alarm Association [CSAA])
- U.S. Department of Justice (DOJ)

In addition, the Respondent's solutions and services shall comply with any additional standards, requirements, statutes, and policies identified throughout this RFP.

**Table 1: Adopted Standards**

| SDO | Standard ID | Standard Title | Standard Description | Latest Revision/ Release Date[1] |
|---|---|---|---|---|
| AICPA | SOC 2 | *System and Organization Controls 2* | Provides a compliance framework used to evaluate and validate an organization's information security practice. | October 2022 |
| APCO/TMA (Formally known as CSAA) ANS | 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* | Provides an assessment tool to evaluate current | Version 3, |

[1] 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[1] |
|---|---|---|---|---|
| | | *(ECC) Service Capability Criteria Rating Scale* | capabilities of the ECC against models representing the best level of preparedness, survivability, and sustainability amidst a wide range of natural and manmade events. | January 30, 2020 |
| 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-1000074.v003 | *Signature-based Handling of Asserted information using toKENs (SHAKEN)* | This document provides telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies to validate legitimate calls and mitigate illegitimate spoofing of telephone identities on IP-based service. | Version 3 August 2022 |
| CIS | CIS Controls | *CIS Critical Security Controls* | Focuses on 18 foundational and advanced cybersecurity actions that address the most prevalent cyber threats. | Version 8.1 June 25, 2024 |
| 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 | Version 6.0 December 27, 204 |

| SDO | Standard ID | Standard Title | Standard Description | Latest Revision/ Release Date[1] |
|---|---|---|---|---|
| | | | criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information. | |
| 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 identifiers and geodetic or civic location information to service contact URIs | August 2008 |
| IETF | RFC 5491 | *GEOPRIV Presence Information Data Format Location Object (PIDF LO) Usage Clarification, Considerations, and Recommendations* | Provides recommendations on how to constrain, represent, and interpret locations in a PIDF-LO | March 2009 |
| IETF | RFC 6341 | *Use Cases and Requirements for SIP-Based Media Recording (SIPREC)* | Specifies requirements for extensions to SIP that will manage delivery of RTP media to a recording device. | August 2011 |
| IETF | RFC 6442 | *Location Conveyance for the Session Initiation Protocol* | Defines an extension to the Session Initiation Protocol | December 2011 |

| SDO | Standard ID | Standard Title | Standard Description | Latest Revision/ Release Date[1] |
|---|---|---|---|---|
| | | | (SIP) to convey geographic location information from one SIP entity to another SIP entity | |
| IETF | RFC 6753 | *A Location Dereference 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 | February 2013 |
| IETF | RFC 7852 | *Additional Data Related to an Emergency Call* | Describes data structures and mechanisms to convey information about an emergency call, caller, or location to the PSAP by value or by reference | July 2016 |
| IETF | RFC 7865 | *Session Initiation Protocol (SIP) Recording Metadata* | Describes the metadata model as viewed by the Session Recording Server (SRS) and the recording metadata format. | May 2016 |
| IETF | RFC 7866 | *Session Recording Protocol* | Specifies the use of the Session Initiation Protocol (SIP), the Session Description Protocol (SDP), and the Real-time Transport Protocol (RTP) for delivering real-time media and metadata from a Communication Session (CS) to a recording device. | May 2016 |
| IETF | RFC 7090 | *Public Safety Answering Point (PSAP) Callback* | Describes a mechanism for marking PSAP callbacks using a new header field value for the SIP Priority header field, called "psap-callback" | April 2014 |
| IETF | RFC 8224 | *Authenticated Identity Management in the Session Initiation Protocol (SIP)* | This document defines a mechanism for securely identifying originators of SIP requests | February 2018 |

| SDO | Standard ID | Standard Title | Standard Description | Latest Revision/ Release Date[1] |
|---|---|---|---|---|
| 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. | January 2021 |
| IETF | RFC 9806 | *Updates to SIP-Based Media Recording (SIPREC) to Correct Metadata Media Type* | Updates RFC 7866 to align with RFC 7865 when labeling recording metadata and also registers the media type. | June 2025 |
| ISO | ISO/IEC 27001:2022 | *Information Security Management Systems* | Provides guidance for establishing, implementing, maintaining and continually improving an information security management system. | Edition 3 October 2022 |
| ISO | ISO/IEC/IEEE 12207:2017 | *Systems and software engineering — Software life cycle processes* | Provides processes that can be employed for defining, controlling, and improving software life cycle processes within an organization or a project. | Edition 1 2017 |
| ISO | ISO/IEC/IEEE 29119-1:2022 | *Software and systems engineering — Software testing Part 1: General concepts* | Defines an internationally agreed set of standards for software testing that can be used by any organization when performing any form of software testing. | Edition 2 2022 |
| NENA | REQ-001.1.2-2018 | *Next Generation 9-1-1 Public Safety Answering Point Requirements* | Provides requirements for functions and interfaces between an i3 PSAP and NGCS, and among functional elements associated with an i3 PSAP | June 10, 2018 |
| NENA | NENA-STA-006.2a-2022 | *NENA Standard for NG9-1-1 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 May 2, 2023 |
| NENA | NENA-STA-008.2-2014 (originally 70-001) | *NENA Registry System Standard* | Describes how registries (lists of values used in NG9-1-1 functional element standards) are created and maintained | October 6, 2014 |

| SDO | Standard ID | Standard Title | Standard Description | Latest Revision/ Release Date[1] |
|---|---|---|---|---|
| NENA | NENA-STA-010.3f-2021 | *NENA i3 Standard for Next Generation 9-1-1* | Builds upon prior NENA publications including i3 requirements and architecture documents and provides additional detail on functional standards | Version 3f December 17, 2024 |
| NENA | NENA-STA-015.10-2018 (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 | NENA-INF-016.2-2018 (formerly 08-506) | *Emergency Services IP Network Design (ESIND) Information Document* | 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 | 54-750 | *NENA/APCO Human Machine Interface & PSAP Display Requirements (ORD)* | Prescribes requirements for the human machine interface (HMI) display for the Next Generation 9-1-1 (NG9- 1-1) System. | Version 1 October 20, 2010 |
| NENA | NENA-STA-040.2-2024 | *NENA Security for Next Generation 9-1-1 Standard (NG-SEC)* | Establishes the minimal guidelines and requirements for levels of security applicable to NG9-1-1 entities | November 4, 2024 |
| NENA | NENA-REF-012.1-2025 | *Security Audit Checklist* | Used to assess compliance with requirements specified in NENA-STA-040.2-2024. | May 6, 2025 |
| 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 | *NENA NG9-1-1 Security (NG-SEC) Information Document* | Provides mechanisms and best practices for cybersecurity for i3 systems | December 8, 2016 |

| SDO | Standard ID | Standard Title | Standard Description | Latest Revision/ Release Date[1] |
|---|---|---|---|---|
| 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-021.1b-2022 | *NENA Standard for Emergency Incident Data Object (EIDO)* | Provides standard format for exchanging emergency incident data between disparate systems and agencies | Version 1b December 17, 2024 |
| NENA | NENA-STA-024.1.1-2025 | *NENA Standard for the Conveyance of Emergency Incident Data Objects (EIDOs) between Next Generation (NG9-1-1) Systems and Applications* | Standard defining how EIDOs are conveyed between Functional Elements | Version 1.1 January 30, 2025 |
| NENA | NENA-STA-031.1-2021 | *NENA Standard for Interconnecting Emergency Services IP Networks and Public Safety Broadband Networks* | Establish standards for interconnections between ESInets and other broadband networks used by first responders | October 14, 2021 |
| NENA | NENA-STA-034.1-2022 | *NENA Legacy Selective Router Gateway (LSRG) Standard* | Provides a technical standard for the LSRG which is a signaling and media connection point between a legacy Selective Router and an i3 ESInet/NGCS | March 17, 2022 |
| NENA / NIOC | NG9-1-1 PKI VP V1.0 | *NG9-1-1 Interoperability Oversight Commission (NIOC) (PSAP) Credentialing Authority (PCA) Certification Validation Guidelines* | Provides the security requirements needed to support the secure validation for issuance of Certificates in NG9-1-1 by the PCA Certification Authorities (CAs) in the NG9-1-1 Public Key Infrastructure. | V1.0.0 February 9, 2022 |
| NENA / NIOC | NG9-1-1 PKI Customer Provided 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 | March 22, 2019 |

| SDO | Standard ID | Standard Title | Standard Description | Latest Revision/ Release Date[1] |
|---|---|---|---|---|
| | | | sensitive but unclassified information | |
| 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 |
| NIST | SP 800-53 | *Security and Privacy Controls for Information Systems and Organizations* | Provides security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks. | Release 5.2.0 August 27, 2025 |
| OWASP | OWASP Top 10:2021 | *OWASP Top 10* | Lists the ten most critical security risks to web applications. | 2021 |
| 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 |

### 5.2.1 Standards Evolution

As industry standards evolve, the Respondent shall upgrade the solution to maintain compliance with the then-current versions of established industry standards.

The solution shall support new IP network, functional, interface, and security industry standards within eighteen (18) months of ratification of the applicable standard.

Compliance obligations shall extend to all supporting standards referenced within each applicable standard.

When updates are implemented to maintain standards compliance, the solution shall not discontinue or materially degrade any services or feature functionality that were available at the time of the upgrade.

The Respondent shall disclose any anticipated performance, configuration, or feature changes prior to implementing the upgrade and shall obtain Customer approval before deployment.

## 5.3 – General Technical Requirements

The Respondent shall support two (2) Emergency Services IP network (ESInet) connectivity configurations, as determined by the 9-1-1 Authority.

Configuration 1 — Respondent-Provided (Respondent Provided): Under the Respondent Provided configuration, the CHE provider shall provide and install CHE connectivity between the NGCS, the CHE interface, and the PSAP.

Configuration 2 — Customer-Provided (Customer Provided): Under the Customer Provided configuration, the ESInet shall be provided by the Customer or 9-1-1 Authority. The Respondent shall use the CP ESInet to connect the CHE solution to the PSAP.

The Respondent shall remain responsible for connectivity between the CHE solution and either the Cloud Instance or the Data Center environment, regardless of whether the Respondent Provided or Customer Provided configuration is used. Where "Respondent Provided" is used, connectivity to the PSAP shall be provided by the CHE provider; where "Customer Provided" is used, connectivity to the PSAP shall be provided by the Customer.

Where neither "Respondent Provided" or "Customer Provided" is specified, the technical requirement shall apply to both configurations.

For clarity, each requirement identified in this section is associated with and shall be interpreted as part of Section 5.3, regardless of the individual Requirement ID numbering shown.

| **5.3.1** | **General** |
|---|---|
| 5.3.1.1 | The implementation of new IP connectivity and the replacement, migration, or rehoming of any part of the Respondent Provided network (including ESInet circuits, phone system, and all other FEs.) shall have the following requirements: |
| 5.3.1.1.1 | The Respondent shall work with the ESInet provider to order, install, and test any new FE circuits needed to connect to the ESInet, as well as collaborate regarding routing specifications (Border Gateway Protocol [BGP], etc.) to accommodate the expected behaviors (load sharing, circuit failover, etc.). |
| 5.3.1.1.2 | Installation and testing activities shall include documented test plans and acceptance results approved by the Customer. |
| 5.3.1.1.3 | The Respondent shall work with Customer representatives to order, install, and test any new circuits, as well as collaborate regarding any expected behaviors therein. |
| 5.3.1.1.4 | The Respondent shall retain end-to-end responsibility for call delivery regardless of third-party involvement from the demarcation point of the NGCS to the PSAP. |
| 5.3.1.1.5 | The Respondent's solution shall provide CHE network connectivity that supports the Customer's current call and data delivery functionality between agencies. |
| 5.3.1.1.6 | Migration activities shall not degrade existing service levels. |
| 5.3.1.1.7 | For a Customer Provided ESInet to the PSAP, the Respondent shall comply with interface and IP addressing scheme, IPv4 and IPv6, as directed by the Customer and shall ensure the bandwidth requirements do not exceed the provided ESInet capabilities. |
| 5.3.1.2 | The Respondent's solution shall have diverse entrance facilities for CHE network connections into the hosted call-handling data centers or cloud instances (Customer Provided and Respondent Provided) as well as into the designated standalone PSAP facilities for an Respondent Provided solution. |
| 5.3.1.2.1 | Diverse entrance facilities shall be physically and logically separate with no common points of failure. |
| 5.3.1.2.2 | Diversity architecture shall be documented and subject to Customer review. |
| 5.3.1.3 | For Respondent Provided: The Respondent shall provide a minimum of one terrestrial (copper or optical circuit) connection Respondent Provided with adequate bandwidth into each PSAP facility (primary and backup) and one additional connection over another physical path to ensure CHE availability. |
| 5.3.1.3.1 | Minimum bandwidth requirements shall be based on busy-hour call and data volumes. |
| 5.3.1.3.2 | Bandwidth adequacy shall be validated during acceptance testing. |

| | |
|---|---|
| 5.3.1.4 | For Respondent Provided: The Respondent shall be capable of receiving and integrating 9-1-1 calls delivered over secondary wireless connections as implemented by the CHE provider (e.g., 5G/Long-Term Evolution [LTE] network, satellite, microwave, carrier-diverse fiber, etc.) and shall be capable of failing over between connections without dropping a 9-1-1 call. |
| 5.3.1.4.1 | Failover between primary and secondary connections shall be automatic and occur within defined recovery time objectives (RTOs). |
| 5.3.1.4.2 | Failover scenarios shall be validated during acceptance testing. |
| 5.3.1.5 | The solution shall align with NENA-STA-010.3f-2021, *Detailed Functional and Interface Specifications for the NENA i3 Solution*, (or its successor document when ratified). |
| 5.3.1.5.1 | Compliance with NENA-STA-010.3f shall be documented and verifiable. |
| 5.3.1.6 | The solution shall use open standards and shall be identified and documented for all major interfaces. |
| 5.3.1.7 | The solution shall support and enforce quality of service (QoS) marking using Differentiated Service Code Point (DSCP). |
| 5.3.1.8 | The solution shall provide network traffic convergence of less than 50 milliseconds (ms). |
| 5.3.1.8.1 | Network convergence and Mean Opinion Score (MOS) metrics shall be measured and reported. |
| 5.3.1.9 | The solution shall maintain an MOS of 4.0. |
| 5.3.1.9.1 | Failure to meet performance thresholds shall constitute a service-impacting issue. |
| 5.3.1.10 | The solution shall scale to support call-volume growth by 50% without requiring replacement of any critical hardware or software component. |
| 5.3.1.10.1 | Scalability requirements shall be validated during load or stress testing. |
| 5.3.1.10.2 | Scalability shall apply throughout the contract term. |
| 5.3.1.11 | Failure of any single instance of a hardware or software element or physical connection shall not impact overall solution performance. |
| 5.3.1.12 | All network-connected elements shall support at least two redundant network interfaces with automatic failover between them and shall be capable of failing over between connections without dropping a 9-1-1 call. |
| 5.3.1.13 | All powered devices supporting network connectivity for the Customer (e.g., firewalls, routers, switches, etc.) shall include a minimum of two redundant power supplies (each shall be capable of powering 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. |
| 5.3.1.13.1 | Any exceptions to redundancy requirements shall require Customer approval. |
| 5.3.1.14 | The Respondent shall provide the ability to log onto the proposed system from an off-site location if the primary PSAP becomes inoperable. |
| 5.3.1.14.1 | Off-site access shall comply with Customer security and authentication policies. |
| 5.3.1.14.2 | Remote access performance shall support full call-handling functionality. |

| **5.3.2** | **Functional Element Solutions Architecture** |
|---|---|
| 5.3.2.1 | If the Respondent supports both a traditional data center-based solution and a cloud-based solution, all technical requirements shall apply to both solution types (data center and cloud). |
| 5.3.2.1.1 | For either a cloud-based solution or a data center solution, the solution shall be:<br>• Managed to ensure the availability meets service level agreement (SLA) requirements<br>• Includes the redundancy needed to meet SLA requirements<br>• Criminal Justice Information Services (CJIS)-compliant<br>• Hosted within North America, inclusive of all parts. |
| 5.3.2.1.2 | The Respondent shall identify the architectural components under the Respondent's direct operational control versus third-party cloud-provider control, including the responsibility for monitoring, incident response, and restoration, upon request from the 9-1-1 Authority. |

| | |
|---|---|
| 5.3.2.1.3 | The solution shall be deployed across multiple physically and logically separate availability zones or fault domains so that no single facility, region, or failure domain can cause a loss of service. |
| 5.3.2.1.4 | The Respondent shall provide the tools needed to support migration of Customer data, configurations, and call records to another hosting environment or provider at contract termination, without service disruption. |
| 5.3.2.2 | The Respondent shall work with the PSAP to coordinate the installation of any hardware and interfaces and shall document all equipment required to be hosted at the emergency communications center (ECC), including purpose, redundancy model, power requirements, network connectivity, and whether each component is optional or mandatory, upon request from the 9-1-1 Authority. |
| 5.3.2.2.1 | Failure or loss of any ECC-hosted equipment shall not prevent call processing, call delivery, or remote call-taking operations. |
| 5.3.2.3 | The Respondent's CHE solution shall interoperate with the Customer's i3-conformant ESInet and NGCS. Until the ESInet/NGCS is available, the Respondent shall identify what IP network the CHE solution shall use in the interim. |
| 5.3.2.3.1 | Any interim IP network used prior to availability of the ESInet/NGCS shall meet the same security, performance, redundancy, and monitoring requirements as the production ESInet-connected environment. |
| 5.3.2.4 | The Respondent shall be responsible for working directly with the ESInet provider to troubleshoot any issues related to call presentations associated with the receipt or transfer of calls through the NGCS provider's ESInet. The Respondent shall update the Customer and any designees weekly, at a minimum, regarding troubleshooting and progress. |
| 5.3.2.4.1 | The Respondent shall retain responsibility for issue coordination and resolution until service is fully restored, regardless of whether the root cause is attributed to the ESInet provider or another third party. |
| 5.3.2.5 | The Respondent shall provide logical and physical architecture diagrams depicting call flow, redundancy, failover, interfaces, and dependency relationships. |
| 5.3.2.6 | The solution architecture shall eliminate all single points of failure. Any remaining unavoidable single dependencies shall be explicitly identified with mitigation strategies. |
| 5.3.2.7 | The architecture shall ensure that no single PSAP, tenant, or agency can exhaust shared system resources to the detriment of other PSAPs. |
| 5.3.2.8 | The Respondent shall limit administrative access paths into the production environment, including how emergency access is controlled, audited, and revoked. |

| **5.3.3** | **Security** |
|---|---|
| 5.3.3.1 | The Respondent shall provide a security in-depth approach that embodies best practices outlined in the latest version of NENA-STA-040.2-2024, *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC),* (or its successor document when ratified). |
| 5.3.3.2 | The Respondent shall include a security plan document that addresses physical, application, and network security. |
| 5.3.3.2.1 | The security plan shall be reviewed and updated at least annually and whenever material architectural or threat changes occur. Updated versions shall be provided to the Customer automatically and on demand. |
| 5.3.3.3 | The solution shall utilize end-to-end encryption for all sensitive data that transits the CHE network (i.e., data in transit), preferably using Advanced Encryption Standard (AES) with a minimum key length of at least 256 bits (AES 256). |

| | |
|---|---|
| 5.3.3.4 | The solution shall encrypt stored data (i.e., data at rest) that contains confidential information using at least AES 256 or an equivalently strong algorithm and shall implement "data at rest" policies such as AES, physical control, strong password requirements, monitoring, and configuration management. |
| 5.3.3.5 | The solution shall support data retention limits that are configurable by the Customer. |
| 5.3.3.5.1 | The solution shall support secure deletion and cryptographic erasure of data at the end of Customer-defined retention periods, including backups and replicas. |
| 5.3.3.6 | If authentication is not fully managed by a third-party identity provider, the solution shall support password security mechanisms for locally managed accounts. The solution shall require that any device or applications with a local account have a password set in accordance with the Authentication/Password Policy before being connected to any Customer system or network. Password security policies shall include the use of strong passwords and defined password expiration and change intervals. Any third-party identify provider used in the solution shall support the same password security mechanisms. |
| 5.3.3.6.1 | Privileged and administrative accounts shall be segregated from standard user accounts and protected with enhanced controls, including mandatory multi-factor authentication (MFA) and session auditing. |
| 5.3.3.7 | The solution shall provide firewalls between call-handling nodes and their external connections. |
| 5.3.3.8 | The Respondent shall ensure that all call-handling components interfacing with ESInet/NGCS provider and FE provided connections carry credentials traceable to the national PSAP Credentialing Agency (PCA). |
| 5.3.3.8.1 | The Respondent shall manage certificate issuance, renewal, revocation, and expiration monitoring for all PCA-issued credentials without service interruption. |
| 5.3.3.9 | The Respondent shall implement single sign-on (SSO), Customer-approved identity providers and MFA in their Functional Element solution to support user access management. The Respondent shall identify all supported SSO and identify provider solutions, including but not limited to Microsoft Azure Active Directory (Azure AD), Active Directory Federation Services [ADFS], or equivalent solutions. |
| 5.3.3.10 | The Respondent shall perform proactive analysis of the network for vulnerabilities including independent security audits of the solution. Analysis and vulnerability scans shall be automated in accordance with a specified schedule, in addition to manual checks. |
| 5.3.3.10.1 | Identified critical and high-risk vulnerabilities shall be remediated within Customer-approved timeframes aligned with severity and service level requirements (SLRs). |
| 5.3.3.11 | The Respondent shall maintain a documented continuity of operations (COOP) plan and a disaster recovery (DR) plan and shall include those plans with its response.<br><br>The Respondent shall review its COOP and DR plans at least annually and shall provide the Customer with either an updated copy of the plans or written confirmation that no changes have occurred, along with the date of the next scheduled review. |
| 5.3.3.11.1 | The Respondent shall test COOP and DR procedures at least annually and provide test results to the Customer. |
| 5.3.3.12 | The Respondent shall provide access reports from facilities (physical access) down to the individual device level (physical or virtual access) upon request, including when a service-impacting issue has occurred. This includes the physical device on which the CHE resides and the components of that device (e.g., the hard drive, power supply, etc.). |

| | |
|---|---|
| 5.3.3.12.1 | Access logs shall be immutable and retained in accordance with Customer-defined retention policies and CJIS requirements. |
| 5.3.3.13 | The Respondent shall support MFA for any access into systems supporting the CHE as well as for access to any externally accessible portals, user interfaces (UIs), system dashboards, etc. |
| 5.3.3.14 | The Respondent shall maintain and update security software policies and procedures addressing both routine maintenance updates and emergency security patches, including antivirus and similar updates. The policy shall define the frequency and maximum turnaround time for each category of updates. The Respondent's security software update policy shall also address update management and end-of-life mitigation for all third-party software components required to support the solution (e.g., Windows Server, OpenSIPS, etc.). |
| 5.3.3.14.1 | Emergency security patches addressing actively exploited vulnerabilities shall be deployed in accordance with Priority 1 service level timelines. |
| 5.3.3.15 | The Respondent shall implement the following cybersecurity and software development standards and their evolving revisions: |
| 5.3.3.15.1 | a. For cybersecurity<br>• NIST Cybersecurity Framework (CSF)<br>• ISO/IEC 27001<br>• CIS Controls<br>• NIST SP 800-53<br>• SOC 2 (for Software as a Service [SaaS]) |
| 5.3.3.15.2 | b. For software development<br>• ISO/IEC 12207<br>• OWASP Top 10<br>• ISO/IEC/IEEE 29119<br>• Development, Security, and Operations (DevSecOps) practices |
| 5.3.3.15.3 | Upon request, the Respondent shall provide audit reports, certifications, or assessment summaries demonstrating alignment with the listed cybersecurity and software development standards. |
| 5.3.3.16 | The Respondent shall complete and submit for approval when awarded the Security Audit Checklist described in NENA-REF-012.1-2025, *Security Audit Checklist*, (or its successor document when ratified).<br>For this procurement, the Respondent shall comply with all identified requirements within the checklist. |
| 5.3.3.17 | The Respondent shall have a documented risk management process, including the use of a standard framework (e.g., NIST CSF) 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. Risk management documentation shall include any third-party risk management processes. |
| 5.3.3.17.1 | Risk assessments shall be reviewed and updated at least annually and following any major incident, architectural change, or threat intelligence update. |
| 5.3.3.18 | The Respondent shall provide when awarded 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. Notification timelines related to cybersecurity breaches shall meet the SLRs described in 5.3.12 of this RFP. |
| 5.3.3.18.1 | The incident response policy shall define notification procedures to affected PSAPs when isolation or containment actions are taken. |
| 5.3.3.19 | The Respondent shall support the ability to isolate specific PSAPs in the event of a cybersecurity breach. |

| | |
|---|---|
| 5.3.3.19.1 | The Respondent shall document criteria and procedures for restoring isolated PSAPs to normal operation following containment. |
| 5.3.3.20 | If a cloud-based solution is proposed, the Respondent shall achieve System and Organization Controls 2 (SOC 2) compliance. |
| 5.3.3.20.1 | SOC 2 Type II reports shall be made available to the Customer upon request, under appropriate confidentiality controls. |
| 5.3.3.21 | The solution shall comply with the latest ratified version of NENA-STA-040.2-2024, *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*. The Respondent shall comply with all portions of the NG-SEC standard and shall be prepared to provide additional details on how the solution complies with standard sections 5.6.3, Device Connectivity; 5.6.7.1, Remote Access Device Security; and 6.17, Remote Access, upon request from the 9-1-1 Authority. |
| 5.3.3.22 | The Respondent shall implement and maintain a security software update policy and associated procedures for the CHE solution. The policy shall define update frequency, including the frequency of antivirus updates, and shall comply with applicable standards and industry best practices. |
| 5.3.3.23 | The Respondent shall comply with independent system security audits applicable to the solution. The Respondent shall also comply with an independent security audit conducted by a third-party auditor selected by the Customer. |
| 5.3.3.23.1 | The Respondent shall remediate audit findings within mutually agreed-upon timelines and provide written confirmation of closure. |

| **5.3.4** | **Functional Element (FE) Network Documentation** |
|---|---|
| 5.3.4.1 | The Respondent shall provide a comprehensive network design, detailing transitional and end-state connectivity for NGCS and FEs, supported by both logical and physical diagrams, call flows, redundancy models, failover paths, demarcation points, and an analysis of single points of failure. |
| 5.3.4.1.1 | Network design documentation shall be version-controlled and updated whenever material changes occur. The current version shall be made available to the Customer upon request. |
| 5.3.4.2 | The Respondent shall provide as-built documentation depicting network paths and equipment diversity, prior to acceptance testing of the solution. |
| 5.3.4.2.1 | As-built documentation shall reflect the deployed production configuration and shall be validated prior to acceptance testing. |
| 5.3.4.2.2 | As-built documentation shall be provided in both read-only and editable formats acceptable to the Customer. |
| 5.3.4.3 | The Respondent shall provide complete network interface specifications for interoperability with FEs, including third-party FEs and neighboring NGCS/ESInets supported by different NGCS providers. Specifications shall include supported protocols, authentication methods, encryption requirements, port usage, version compatibility, and any required certificates or trust models. |
| 5.3.4.3.1 | The Respondent shall notify the Customer in advance of any changes to network interfaces or specifications that may affect interoperability. |
| 5.3.4.4 | The Respondent shall provide detailed as-built solution documentation for the implemented production environment and all associated backup, DR, and testing environments (as applicable). Documentation shall include network, equipment, and cloud architecture information, including network paths, network providers, BGP information, firewalls, availability zones, software versions, and all configured parameters representing the implemented design. |
| 5.3.4.4.1 | As-built documentation shall include dependency mappings between network components, applications, cloud services, and third-party providers. |

| | |
|---|---|
| 5.3.4.4.2 | As-built documentation shall identify all security-relevant components, including firewalls, access controls, certificate authorities, logging systems, and monitoring integrations. |
| 5.3.4.5 | The Respondent shall provide all required documentation within Customer-defined timeframes prior to acceptance testing and update documentation within thirty (30) days of any approved change. |
| 5.3.4.6 | The Respondent shall certify that all documentation accurately reflects the deployed solution at the time of delivery. |
| 5.3.4.7 | Documentation shall be made available to the Customer in a secure, centralized repository with controlled access. |
| 5.3.4.8 | The Respondent shall retain historical versions of documentation for the duration of the contract and make them available to the Customer upon request. |

| **5.3.5** | **Monitoring and Alarming** |
|---|---|
| 5.3.5.1 | The Respondent shall provide physical access monitoring and reporting for all facilities where the software running the call-handling service resides. |
| 5.3.5.1.1 | Physical access logs shall be retained in accordance with Customer-defined retention requirements and correlated with service-affecting events and incidents when applicable. |
| 5.3.5.2 | The Respondent shall provide automated monitoring and alarming for all network nodes and software instances supporting the solution. Monitoring and alarming shall occur in real or near-real time, with a refresh interval not exceeding sixty (60) seconds for critical components. |
| 5.3.5.3 | User access logs shall capture authentication attempts, role changes, privilege elevation, account creation, modification, and deletion. |
| 5.3.5.4 | The solution shall support logging of administrative and audit events. These logs must be immutable. |
| 5.3.5.4.1 | Immutable audit logs shall be protected from alteration or deletion and retained in accordance with Customer-defined retention requirements and CJIS standards. |
| 5.3.5.5 | The Respondent shall provide event logging, including call status information such as mute, on-hold, and transfer, and reporting in real or near-real time. |
| 5.3.5.5.1 | All logged events shall include synchronized timestamps aligned with system time synchronization requirements defined elsewhere in this RFP. |
| 5.3.5.6 | The Respondent shall provide FE network monitoring and alerting (regardless of whether the network is new or existing) and act on the alerts according to the level of impact on the FE service and in accordance with SLAs. |
| 5.3.5.6.1 | Alerts shall be classified by severity and mapped to response and escalation timelines consistent with SLRs. |
| 5.3.5.7 | The Respondent shall provide FE hardware and software monitoring and alerting, and act on the alerts according to the level of impact on the FE service and in accordance with SLAs. |
| 5.3.5.7.1 | Monitoring systems shall support proactive detection of performance degradation, capacity exhaustion, and anomalous behavior prior to service impact. |
| 5.3.5.8 | The Respondent shall provide user-definable and user-changeable notification levels and recipients with text and email delivery options. |
| 5.3.5.8.1 | Notification capabilities shall support escalation chains, acknowledgment tracking, and failover notification paths if primary recipients do not respond. |
| 5.3.5.9 | The executive dashboard shall provide real-time visibility into alarms, incidents, and system health, and shall support role-based access for Customer and Respondent personnel. |
| 5.3.5.10 | The Respondent shall provide the ability to replicate select alerts to a third-party monitoring and reporting system. |

| | |
|---|---|
| 5.3.5.10.1 | Alert replication to third-party systems shall use secure, authenticated interfaces and comply with Customer security requirements. |
| 5.3.5.11 | The Respondent shall support Simple Network Management Protocol (SNMP) for monitoring and managing network devices and applications on the IP-based CHE network. SNMP support shall use secure versions (SNMPv3) with authentication and encryption enabled. Use of SNMPv1 or SNMPv2c shall not be permitted. |
| 5.3.5.12 | The Respondent shall support syslog as the standard protocol and architecture for logging messages associated with events/alarms from various devices and applications. These messages shall be sent to a centralized syslog server for storage, monitoring, and analysis. |
| 5.3.5.12.1 | Centralized syslog data shall be normalized and made available for integration with security information and event management (SIEM) platforms. |
| 5.3.5.13 | The solution shall support searchable log retention based on Customer-defined timeframes and allow filtering by PSAP, user, system component, and event type. |
| 5.3.5. 14 | Customer personnel shall have read-only access to monitoring dashboards, alerts, and logs relevant to their PSAPs. |
| 5.3.5.15 | The Respondent shall support the periodic testing of monitoring and alerting mechanisms to validate delivery, escalation, and response workflows. |
| 5.3.5.16 | The Respondent shall certify that all CHE components, including third-party dependencies, are included in monitoring coverage. |

| **5.3.6** | **Network Operation Center (NOC)/Security Operations Center (SOC)** |
|---|---|
| 5.3.6.1 | The Respondent shall provide a 24/7/365 staffed NOC and/or SOC located within North America. A primary and backup NOC/SOC shall be maintained. The backup shall be hot (preferred) or warm and shall be geographically and operationally independent such that a single facility failure, regional outage, cyber event, or staffing disruption cannot impact both centers simultaneously. |
| 5.3.6.1.1 | The Respondent shall always maintain sufficient qualified staffing to meet response and escalation timelines defined in this RFP. |
| 5.3.6.2 | The Respondent shall provide the ability for users to submit, track, and modify tickets by phone, email, and any direct IT service management (ITSM) user access that may be available for incidents, problems, changes, and maintenance. |
| 5.3.6.2.1 | Customer personnel shall have real-time visibility into ticket status, history, priority, and assigned resources via the ITSM system. |
| 5.3.6.3 | The Respondent shall provide outward notifications and updates of customer tickets via phone, email, and text. Notifications shall be issued at ticket creation, status change, escalation, and resolution, and at intervals aligned with severity-based update requirements. |
| 5.3.6.4 | The Respondent shall provide fully documented escalation procedures when awarded with contact information for all primary and secondary responsible personnel at all levels of escalation. |
| 5.3.6.4.1 | During escalated incidents, the Respondent shall provide status updates at intervals consistent with Priority 1 and Priority 2 escalation requirements. |
| 5.3.6.4.2 | Escalation procedures shall identify decision-making authority at each escalation level. |
| 5.3.6.5 | The Respondent shall provide Reason for Outage (RFO) reports and regulatory compliance reporting in accordance with Federal Communications Commission (FCC) requirements. |
| 5.3.6.5.1 | For Priority 1 and Priority 2 incidents, interim status reports shall be provided to the Customer until the final RFO and root cause analysis are delivered. |

| | |
|---|---|
| 5.3.6.6 | Preliminary RFO reports are due to the Customer within five (5) business days of the initial issue report; final root cause analysis is due within fourteen (14) calendar days of root cause determination, including steps taken to prevent the issue from recurring. |
| 5.3.6.6.1 | The Customer shall have the right to review, comment on, and request clarification or revision of RFO and root cause analysis reports. |
| 5.3.6.7 | The Respondent shall provide a media role contact for any outage or service interruption or failure. The Customer shall be informed immediately of any changes in contact information. |
| 5.3.6.7.1 | Each media role shall include a designated primary and secondary contact available 24/7/365. |
| 5.3.6.8 | The Respondent shall provide a governance contact for any outage or service failure. The Customer shall be informed immediately of any changes in contact information. |
| 5.3.6.8.1 | Each governance role shall include a designated primary and secondary contact available 24/7/365. |
| 5.3.6.9 | The Respondent shall provide a service management contact for any outage or service failure. The Customer shall be informed immediately of any changes in contact information. |
| 5.3.6.9.1 | Each service management role shall include a designated primary and secondary contact available 24/7/365. |
| 5.3.6.10 | The Respondent shall provide access to technical and executive staff for escalations. |
| 5.3.6.10.1 | Technical and executive escalation resources shall be available within timeframes consistent with escalation requirements defined in this RFP. |
| 5.3.6.11 | The Respondent shall provide NOC/SOC staff who are trained and experienced in 9-1-1 operations and shall maintain regular refresher and update training plans for such staff. |
| 5.3.6.11.1 | The Respondent shall document NOC/SOC training programs and conduct refresher training at least annually. Training records shall be made available to the Customer upon request. |
| 5.3.6.12 | The Respondent shall provide the ability to access, troubleshoot, diagnose, and repair network and systems remotely. |
| 5.3.6.12.1 | Remote access for troubleshooting shall use secure, authenticated connections with session logging and approval controls. |
| 5.3.6.13 | 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). |
| 5.3.6.13.1 | The Respondent shall provide supporting artifacts (e.g., call traces, logs, packet captures) to demonstrate reasonable assistance efforts when issues originate outside the Respondent's solution. |
| 5.3.6.14 | The Respondent shall define an incident command structure for managing Priority 1 and Priority 2 incidents, including roles, responsibilities, and communication paths. |
| 5.3.6.15 | For Priority 1, the Respondent shall provide periodic reporting on NOC/SOC performance, including response times, resolution times, escalation frequency, and SLA compliance. |
| 5.3.6.16 | For Priority 2 incidents, the Respondent shall conduct a post-incident review with the Customer to review root cause, response effectiveness, and corrective actions. |

| | |
|---|---|
| 5.3.6.17 | Customers shall have the right to participate in incident bridge calls and post-incident reviews for service-affecting events. |

| **5.3.7** | **Industry Standards Evolution** |
|---|---|
| 5.3.7.1 | As industry standards evolve, the solution shall be upgraded to maintain conformance with the then-current version of applicable industry standards. The solution shall support new call-handling and security standards within eighteen (18) months of ratification. Conformance obligations shall extend to all supporting or referenced standards incorporated within each applicable standard. |
| 5.3.7.2 | Applicable industry standards shall include, at a minimum, NENA, IETF, ATIS, ISO/IEC, NIST, CJIS, and FCC-mandated standards relevant to FE functionality, security, and interoperability. |
| 5.3.7.2.1 | The Respondent shall notify the Customer when a newly ratified or updated industry standard materially impacts the solution and identify whether and how conformance will be achieved. |
| 5.3.7.2.2 | If full conformance cannot be achieved within the specified timeframe, the Respondent shall provide a written remediation plan identifying interim measures, risks, and target compliance dates. |
| 5.3.7.2.3 | Upgrades required solely to maintain conformance with applicable industry standards shall be provided without additional licensing or subscription fees beyond those defined in a resulting contract. |
| 5.3.7.3 | 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 the Customer for approval. |

| **5.3.8** | **Regulatory and i3 Standards Conformance** |
|---|---|
| 5.3.8.1 | The solution shall conform to the latest published/ratified version of NENA-STA-010.3f-2021, *NENA i3 Standard for Next Generation 9-1-1*. |
| 5.3.8.1.1 | The solution shall not remove, materially degrade, or reduce the performance, capacity, or availability of services, features, or functionality in place at the time of upgrade. |
| 5.3.8.1.2 | Prior to deployment of any upgrade, the Respondent shall provide release notes and validation results demonstrating continued compliance with existing requirements. |
| 5.3.8.1.3 | The Respondent shall support rollback to the prior production version in the event of a service-affecting issue introduced by an upgrade. |
| 5.3.8.1.4 | Customer approval of performance or feature changes shall be obtained prior to production deployment, except in the case of emergency security patches. |
| 5.3.8.2 | The solution shall interface with any NENA i3-conformant NGCS and ESInet. |
| 5.3.8.2.1 | The solution shall provide all signaling, response data, and information needed to support all NGCS FEs. |
| 5.3.8.2.2 | The Respondent shall demonstrate interoperability with multiple i3-conformant NGCS and ESInet implementations without proprietary extensions. |
| 5.3.8.2.3 | The solution shall interoperate with NGCS and ESInet environments operating different, but overlapping, i3 standard versions during transition periods. |
| 5.3.8.3 | The Respondent's solution shall support the use of Presence Information Data Format Location Object (PIDF-LO), Emergency Incident Data Object (EIDO), Hypertext Transfer Protocol (HTTP)-enabled location delivery (HELD), Location-to-Service Translation (LoST), Additional Data Repository (ADR) queries, and other i3 protocols. |

| | |
|---|---|
| 5.3.8.4 | The solution shall function in a legacy 9-1-1 network environment during the transition to i3 NGCS and ESInet infrastructure. |
| 5.3.8.4.1 | The solution shall support legacy 9-1-1 interoperability for the duration of the Customer's transition to an i3 NGCS and ESInet, as determined by the Customer. |
| 5.3.8.4.2 | During transition, the solution shall maintain functional parity for call handling, routing, and logging, to the extent technically feasible. |
| 5.3.8.5 | The Respondent shall provide a written attestation of compliance with all applicable regulatory and i3 requirements at the time of system acceptance. |
| 5.3.8.6 | The Respondent shall notify the Customer of material regulatory or standards changes that impact the solution and describe the required remediation approach during the duration of the contract period. |
| 5.3.8.7 | Any known non-conformances or partial implementations of regulatory or i3 requirements shall be disclosed with mitigation plans and timelines at the time of contract signing and throughout the duration of the contract upon discovery. |

| **5.3.9** | **FE Technical Support** |
|---|---|
| 5.3.9.1 | The Respondent shall provide a 24/7/365 NOC/SOC for reporting and escalating software and hardware issues. NOC/SOC Tier 1 and 2 personnel shall be based in North America. |
| 5.3.9.1.1 | The Respondent shall define Tier 1 through Tier 4 support responsibilities, authority, and escalation criteria, including engagement of Tier 3 and Tier 4 engineering resources, and shall provide documentation of such processes upon request. |
| 5.3.9.1.2 | Tier 3 and Tier 4 technical support resources shall be available 24/7/365 for Priority 1 and Priority 2 incidents. |
| 5.3.9.1.3 | Each support tier shall have clearly identified roles and escalation authority aligned with the SLRs found in Appendix A. |
| 5.3.9.2 | The Respondent shall provide a maintenance plan outlining compliance with the requirements contained in 5.3 upon request. |
| 5.3.9.3 | Upon identification of an issue, the Respondent shall adhere to the timelines for response, repair, and escalation intervals provided in Appendix A. |
| 5.3.9.3.1 | The Respondent shall track, measure, and report compliance with response, repair, and escalation timelines defined in Appendix A. |
| 5.3.9.3.2 | SLA measurement shall begin at ticket creation or automated alert generation, whichever occurs first. |
| 5.3.9.4 | The Respondent shall provide a redundant/secondary/backup NOC/SOC or equivalent to support capabilities and capacity in the event the primary center is offline or otherwise unusable. |
| 5.3.9.4.1 | The backup NOC/SOC shall be fully capable of assuming all operational responsibilities of the primary center, including monitoring, escalation, and customer communication. |
| 5.3.9.4.2 | The primary and backup NOC/SOC shall be geographically and operationally independent. |
| 5.3.9.5 | The Respondent shall provide onsite technical support to address issues with any vendor as related to integration-provided hardware or software that may be installed at Customer facilities. Such support may include responding to system alarms, repairing workstations, routers, or firewalls, and troubleshooting system outages. Onsite technical support shall be provided in accordance with the agreed repair time SLAs. |
| 5.3.9.5.1 | The Respondent shall provide documentation, upon request, that defines conditions under which onsite technical support will be dispatched, including severity thresholds and maximum dispatch times. |

| | |
|---|---|
| 5.3.9.5.2 | Onsite support shall include troubleshooting of interfaces between vendor-as related to integration provided components and Customer or third-party systems, to the extent required to restore service. |
| 5.3.9.6 | The Respondent shall support real-time collaboration with Customer personnel using Customer-approved collaboration tools during incident investigation and resolution. |
| 5.3.9.6.1 | For Priority 1 and Priority 2 incidents, the Respondent shall establish and maintain incident bridge calls until service restoration. |
| 5.3.9.7 | 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). |
| 5.3.9.7.1 | The NOC/SOC COOP plan shall be tested at least annually, and test results shall be made available to the Customer upon request |
| 5.3.9.7.2 | The COOP plan shall ensure uninterrupted monitoring, escalation, communication, and technical support capabilities during remote or degraded operations. |
| 5.3.9.8 | The Respondent shall maintain and use documented troubleshooting procedures and knowledge bases for recurring call-handling issues. |
| 5.3.9.9 | Customer personnel shall be permitted to participate in troubleshooting sessions and post-incident reviews for service-affecting issues. |
| 5.3.9.10 | For Priority 1 and Priority 2 incidents, the Respondent shall conduct a post-incident review addressing root cause, response effectiveness, and corrective actions. |
| 5.3.9.11 | The Respondent shall provide periodic reporting on technical support performance, including ticket volume, response times, escalation frequency, and SLA compliance. |

| **5.3.10** | **Solution Validation** |
|---|---|
| 5.3.10.1 | At the discretion of the Customer, the Respondent shall allow for independent third-party validation of all mandatory solution requirements and feature functionality prior to cutover of the site(s). |
| 5.3.10.1.1 | Independent validation may include functional, performance, security, interoperability, and resilience testing, and the Respondent shall fully cooperate with the selected third party. |
| 5.3.10.1.2 | The Respondent shall remediate any deficiencies identified during independent validation prior to cutover, unless otherwise approved by the Customer. |
| 5.3.10.2 | The solution shall provide transparency and access to all Session Initiation Protocol (SIP) messaging, call detail records (CDRs), key performance indicators (KPIs) (e.g., MOS, delay, jitter, packet loss), data/call logs, and any other data determined to be necessary to verify compliance with contractual obligations or to troubleshoot issues. |
| 5.3.10.2.1 | Transparency and access shall include both real-time and historical data sufficient to support validation, auditing, and root cause analysis. |
| 5.3.10.2.2 | The solution shall support export of validation and troubleshooting data in non-proprietary formats acceptable to the Customer. |
| 5.3.10.3 | The Respondent shall use Customer-designated training workstations for integration, smoke testing, bug fixes, feature validation, and method of procedure verification prior to production deployment. |
| 5.3.10.3.1 | The solution shall clearly identify, segregate, and prevent test calls from impacting live call-handling operations. |
| 5.3.10.4 | The Respondent shall provide documentation of completed results from testing of any hardware or software changes in the Training room. |

| | |
|---|---|
| 5.3.10.4.1 | Test result documentation shall include traceability to specific requirements, test cases, and acceptance criteria. |
| 5.3.10.4.2 | Test documentation shall be retained for the duration of the contract and made available to the Customer upon request. |
| 5.3.10.5 | 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 the Customer within three months of contract signature. The Customer will review and determine acceptance or modification of the test suite. |
| 5.3.10.5.1 | The test suite shall be updated to reflect solution changes, standards evolution, and requirement modifications, subject to Customer approval. |
| 5.3.10.5.2 | Each test case shall include clearly defined acceptance criteria and objective pass/fail determinations. |
| 5.3.10.6 | The Respondent shall perform regression testing following any hardware, software, or configuration change and provide documented results to the Customer prior to production deployment. |
| 5.3.10.7 | The solution shall support performance, load, and stress testing that validates compliance with scalability, latency, and failover requirements defined in this RFP. |
| 5.3.10.8 | Final acceptance of validation and test results shall reside solely with the Customer. |
| 5.3.10.9 | Prior to cutover, the Respondent shall certify that all mandatory requirements have been validated and accepted. |

| **5.3.11** | **Multi-Tenant Capability** |
|---|---|
| 5.3.11.1 | Each tenant shall be logically isolated such that configuration changes, failures, security events, or performance degradation in one tenant do not impact any other tenant. |
| 5.3.11.1.1 | The solution shall support controlled transition of training workstations to live call-taking mode, with safeguards to prevent accidental routing of test calls into live operations. |
| 5.3.11.1.2 | The solution shall support the addition of new tenants without requiring system downtime or reconfiguration of existing tenants. |
| 5.3.11.2 | The Customer's technical personnel 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, greetings, etc.); individual customization for a single user to support Americans with Disabilities Act (ADA) requirements shall be accommodated. |
| 5.3.11.2.1 | Tenant-specific configurations shall be independent and shall not be overridden by system-wide changes without Customer approval. |
| 5.3.11.2.2 | Individual ADA-related user configurations shall persist across software upgrades, configuration changes, and tenant modifications. |
| 5.3.11.2.3 | All tenant-level and user-level configuration changes shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.11.3 | Authorized Customer administrative personnel shall have real-time and historical visibility into configuration, performance metrics, alarms, logs, and reports on a per-PSAP or per-tenant basis. |
| 5.3.11.3.1 | Visibility and control shall be governed by role-based access controls to ensure administrators only access authorized tenants and PSAPs. |
| 5.3.11.4 | The solution shall support centralized administrative access that allows authorized Customer personnel to manage multiple tenants without logging into each tenant individually. |

| | |
|---|---|
| 5.3.11.4.1 | The solution shall provide confirmation prompts, change previews, and rollback capabilities for administrative actions that affect multiple tenants. |
| 5.3.11.4.2 | Administrative interfaces shall clearly indicate the scope and impact of changes before execution, including which tenants and PSAPs are affected. |
| 5.3.11.5 | Each tenant shall have independent security controls, credentials, certificates, and audit logs, aligned with Section 5.3.3, Security, requirements. |
| 5.3.11.6 | Monitoring, alerting, and reporting shall be available on a per-tenant and per-PSAP basis in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.11.7 | The solution shall support backup, restoration, and recovery operations on a per-tenant basis without impacting other tenants. |
| 5.3.11.8 | The Respondent shall support secure provisioning, modification, suspension, and decommissioning of tenants, including secure data retention or destruction as directed by the Customer. |

| **5.3.12** | **System Availability** |
|---|---|
| 5.3.12.1 | The solution shall automatically (i.e., without manual intervention) transfer or failover core processing functionality from one system to another (i.e., "hot" recovery site) upon detection of a problem that impacts the system's ability to meet the 99.999% SLR.<br>Note: For Customer Provided connectivity, this requires the ESInet and NGCS to be operational. |
| 5.3.12.1.1 | Automatic failover shall be triggered based on defined health checks and performance thresholds that indicate the solution cannot meet the 99.999%. |
| 5.3.12.1.2 | Automatic failover shall occur within Customer-defined RTOs without operator intervention. |
| 5.3.12.2 | 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 resynchronize once a problem is corrected. |
| 5.3.12.2.1 | Manual recovery actions shall be restricted to authorized personnel and logged in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.12.2.2 | Following recovery and resynchronization, the Respondent shall validate system integrity and performance prior to returning to normal operations. |
| 5.3.12.3 | The Respondent shall ensure the solution achieves 99.999% availability. |
| 5.3.12.3.1 | The Respondent shall demonstrate how the solution achieves 99.999% availability through documented architecture, redundancy, failover testing, and historical performance metrics. |
| 5.3.12.3.2 | Availability calculations shall be defined, including inclusions, exclusions, and measurement methodology, and aligned with service level definitions found in Appendix A. |
| 5.3.12.4 | The solution shall support distribution of core-processing functionality across two or more systems provided by the Respondent or the Customer. |
| 5.3.12.4.1 | Distributed core-processing components shall be deployed in geographically and operationally independent locations to eliminate single points of failure. |
| 5.3.12.5 | Each FE solution shall have sufficient configured capacity to support at least 125% of busy-hour based on yearly trend 9-1-1 call volume with no loss of service. |
| 5.3.12.5.1 | Capacity assumptions and busy-hour calculations shall be documented and validated during acceptance testing and periodically thereafter. |
| 5.3.12.5.2 | Each FE solution shall support the required capacity during single-site failure scenarios. |
| 5.3.12.6 | The FE solution shall support secure remote solution access using Respondent-provided and -maintained laptops over a virtual private network (VPN) or other Customer-approved broadband connections. |

| | |
|---|---|
| 5.3.12.6.1 | Remote solution access shall comply with Section 5.3.3, Security, requirements, including MFA, device controls, and session logging. |
| 5.3.12.7 | The Respondent shall conduct annual failover and recovery testing and provide documented results to the Customer. |
| 5.3.12.8 | System availability requirements shall apply during large-scale incidents, disasters, and special events involving multi-PSAP operations. |
| 5.3.12.9 | Failure to meet the 99.999% availability requirement shall be subject to service level remedies as defined in Appendix A. |

| **5.3.13** | **Long-Term Availability** |
|---|---|
| 5.3.13.1 | The Respondent shall provide twelve (12) months' (minimum) advance written notification to the Customer 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. |
| 5.3.13.1.1 | Replacement and mitigation plans for EOL/EOS components shall be subject to Customer review and approval prior to implementation. |
| 5.3.13.1.2 | Replacement of EOL/EOS components required to maintain contractual functionality and compliance shall not result in additional licensing or subscription costs beyond those defined in a resulting contract. |
| 5.3.13.2 | The Respondent shall report EOL for any product used in the Respondent's solution that is not controlled by the CHE Respondent. |
| 5.3.13.2.1 | The Respondent shall notify the Customer of third-party product EOL/EOS within thirty (30) days of the Respondent becoming aware of such status. |
| 5.3.13.2.2 | EOL/EOS notifications shall include an impact assessment identifying operational, security, and compliance risks. |
| 5.3.13.3 | The proposed solution shall be supported by the respondent for a minimum of five (5) years from the date of full system acceptance by the Customer(plus any optional contract extensions). |
| 5.3.13.3.1 | "Supported" shall mean full manufacturer support, including security updates, bug fixes, compatibility updates, and access to technical assistance. |
| 5.3.13.3.2 | Support obligations shall extend through the full term of the base contract and any exercised contract extensions. |
| 5.3.13.4 | The Respondent shall provide a product and technology lifecycle roadmapwhen awarded identifying expected support timelines and planned major upgrades affecting the solution. |
| 5.3.13.5 | The Respondent shall support planned technology refresh activities without service interruption and in alignment with Section 5.3.12, System Availability, requirements. |
| 5.3.13.6 | The Respondent shall maintain an obsolescence management process to proactively identify and mitigate long-term availability risks. |
| 5.3.13.7 | Any replacement of EOL/EOS components shall be subject to validation and acceptance testing in accordance with Section 5.3.10, Solution Validation. |

| **5.3.14** | **Computer-aided Dispatch (CAD) System Interoperability** |
|---|---|
| 5.3.14.1 | The solution shall support the CAD system interface as described in NENA-STA-027.3-2025, *NENA E9-1-1 PSAP Equipment Standards*. The solution shall support the latest ratified version of the standard throughout the life of the service. |
| 5.3.14.1.1 | The Respondent shall provide a requirement-by-requirement compliance matrix when awarded demonstrating conformance with NENA-STA-027.3-2025 and its successor standards. |

| | |
|---|---|
| 5.3.14.1.2 | Updates required to maintain conformance with successor versions of the CAD interoperability standard shall be provided in accordance with Section 5.3.7, Industry Standards Evolution, and without additional licensing fees. |
| 5.3.14.2 | The solution shall support NG9-1-1 functionality that includes the delivery of Additional Data, including text, imagery, and video conveyed in an EIDO "by value" or "by reference" to the CAD system (or NG9-1-1 functional equivalent). |
| 5.3.14.3 | Delivery of Additional Data and EIDOs to the CAD system shall be reliable, ordered, and correlated via the available up to date standard to the originating call or incident. |
| 5.3.14.3.1 | EIDOs shall be formatted as defined in NENA-STA-021.1b-2022, *NENA Standard for Emergency Incident Data Object (EIDO)*, (or its successor document when ratified). |
| 5.3.14.3.2 | The solution shall support backward compatibility with prior EIDO versions during transition periods where required by the Customer. |
| 5.3.14.3.3 | The interface used for EIDO conveyance shall conform to NENA-STA-024.1.1-2025, *Conveyance of Emergency Incident Data Objects (EIDOs) between Next Generation (NG9-1-1) Systems and Applications*, or its successor. |
| 5.3.14.3.4 | Any proprietary APIs used for EIDO conveyance shall be fully documented, versioned, and provided without additional licensing fees. |
| 5.3.14.3.5 | If Additional Data delivery to the CAD system fails, the FE solution shall retain and retry delivery and alert operators in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.14.4 | The solution shall support both serial and IP-based connections to a CAD system. |
| 5.3.14.4.1 | IP-based connections shall follow i3 standards related to the use of the United States Civic Location Data Exchange Format (CLDXF-US) (NENA-STA-004.2-2024, *NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF-US) Standard*, or its successor document when ratified) and shall support CAD-related logging events. |
| 5.3.14.4.2 | IP-based CAD system connections shall be encrypted, authenticated, and logged in accordance with Section 5.3.3, Security, requirements. |
| 5.3.14.4.3 | CAD-related events and updates shall be delivered within defined latency thresholds suitable for real-time dispatch operations. |
| 5.3.14.5 | The solution shall support bidirectional import and export of phone book data between FE solutions and the CAD system without data loss. |
| 5.3.14.5.1 | The Respondent shall define when awarded conflict detection and resolution mechanisms when synchronizing phone book data. |
| 5.3.14.6 | The solution shall support automated, near-real-time data transfer between the FE solution and CAD, including call details, location, and incident updates. All interfaces, APIs, scripts, configuration, development, integration, testing, and support required to meet this requirement shall be included in the base solution and shall not result in any additional cost to the Customer. |
| 5.3.14.6.1 | Supported data elements and integration shall be explicitly identified and documented. |
| 5.3.14.7 | The solution shall support resynchronization of call and incident data with CAD systems following outages or connection loss. |
| 5.3.14.7.1 | Resynchronization shall preserve data integrity, timestamps, and event sequencing. |
| 5.3.14.7.2 | Resynchronization actions shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.14.7.3 | The solution shall support resynchronization of CAD data for Customer-defined outage durations. |
| 5.3.14.8 | The solution shall support interoperability with multiple CAD systems used by the Customer or neighboring agencies. |

| | |
|---|---|
| 5.3.14.9 | CAD system interface health, failures, and performance shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.14.10 | CAD system interoperability shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |
| 5.3.14.11 | The Customer shall retain ownership of all CAD-related data exchanged with the CHE solution. |

| **5.3.15** | **Location Information Server (LIS)/Location Database (LDB)** |
|---|---|
| 5.3.15.1 | The solution shall support interface(s) with the LIS as defined in NENA-STA-010.3f-2021, *NENA Detailed Functional and Interface Standards for the NENA i3 Solution*, and the LDB as defined in NENA-INF-008.1, *NENA NG9-1-1 Transition Plan Considerations Information Document,* (or their successor documents once published). |
| 5.3.15.1.1 | The solution shall maintain conformance with successor versions of applicable LIS and LDB standards in accordance with Section 5.3.7, Industry Standards Evolution. |
| 5.3.15.1.2 | The Respondent shall identify operational deployments where the proposed solution interoperates with i3-compliant LIS and/or LDB implementations. |
| 5.3.15.2 | The solution shall support manual initiation of HELD location dereference queries by authorized telecommunicators. |
| 5.3.15.2.1 | Manual HELD dereference actions shall be restricted to authorized users and logged in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.15.2.2 | Results of manual HELD dereference queries shall be presented to the telecommunicator in near-real time and integrated into the active call record. |
| 5.3.15.3 | The solution shall support any transition period during which an LDB and i3-compliant LIS services may need to be accessed by the call-handling solution. |
| 5.3.15.3.1 | The solution shall support concurrent access to LDB and i3-compliant LIS services during transition periods without service degradation or data loss. |
| 5.3.15.3.2 | The solution shall define and enforce prioritization and fallback logic between LDB and LIS data sources during transition periods. |
| 5.3.15.3.3 | The solution shall identify, flag, and log discrepancies between LDB and LIS location data. |
| 5.3.15.4 | The solution shall support dynamic updates to location information during an active call and propagate updates to mapping and CAD systems. |
| 5.3.15.5 | LIS and LDB connectivity, query success, latency, and failures shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.15.6 | Access to LIS and LDB services shall comply with Section 5.3.3, Security, requirements, including encryption, authentication, and audit logging. |
| 5.3.15.7 | LIS and LDB interoperability shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |
| 5.3.15.8 | The Customer shall retain ownership of all location data accessed or processed by the CHE solution, and such data shall be retained and protected in accordance with Customer policy. |

| **5.3.16** | **Additional Data/Emergency Incident Data Object (EIDO)** |
|---|---|
| 5.3.16.1 | The solution shall support a SIP interface from the ESInet/NGCS that includes Additional Data conveyed “by reference” and “by value.” |
| 5.3.16.1.1 | Failure to receive or dereference Additional Data shall not block call presentation and shall generate alerts in accordance with Section 5.3.5, Monitoring and Alarming. |

| | |
|---|---|
| 5.3.16.2 | The solution shall support interface(s) with Additional Data Repositories (ADRs) as defined in NENA-STA-010.3f-2021, *NENA Detailed Functional and Interface Standards for the NENA i3 Solution*, (or its successor document, once published/ratified) to facilitate the dereferencing of Additional Data that is conveyed "by reference." |
| 5.3.16.2.1 | Dereferencing of Additional Data via ADRs shall occur within Customer-defined latency thresholds suitable for live call handling. |
| 5.3.16.2.2 | The solution shall support redundancy and failover for ADR connectivity where available. |
| 5.3.16.3 | The solution shall support the creation of EIDOs as defined in NENA-STA-021.1b-2022, *NENA Standard for Emergency Incident Data Object (EIDO),* (or its successor document, once published/ratified) and the conveyance of EIDOs "by value" and "by reference" between functional components of the solution, and "by reference" between PSAPs/agencies during call transfer. |
| 5.3.16.3.1 | EIDOs shall preserve data integrity, schema compliance, versioning, and timestamps throughout creation and conveyance. |
| 5.3.16.3.2 | Conveyance of EIDOs between functional components shall include CHE, CAD, mapping, recording, analytics, and inter-PSAP transfers where applicable. |
| 5.3.16.3.3 | EIDO transfer between PSAPs/agencies shall enforce tenant, PSAP, and role-based access controls in accordance with Sections 5.3.11, Multi-Tenant Capability, and 5.4.7, CHE User Profiles. |
| 5.3.16.4 | The solution shall support an HTTPS GET interface to facilitate the dereferencing of EIDOs that are received "by reference." |
| 5.3.16.4.1 | HTTPS GET dereferencing of EIDOs shall require authentication and authorization consistent with Section 5.3.3, Security, requirements. |
| 5.3.16.4.2 | EIDO dereferencing requests and responses shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.16.5 | Additional Data and EIDO receipt, dereferencing, failures, and latency shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.16.6 | The Customer shall retain ownership of all Additional Data and EIDO content processed by the solution, and such data shall be retained and protected in accordance with Customer-defined policies. |
| 5.3.16.7 | The solution shall support backward compatibility with prior versions of EIDO and Additional Data standards during transition periods. |
| 5.3.16.8 | Additional Data and EIDO functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.3.17** | **Human Machine Interface (HMI)** |
|---|---|
| 5.3.17.1 | The solution shall comply with NENA 54-750, *NENA/APCO Human Machine Interface & PSAP Display Requirements* (or its successor document when ratified). |
| 5.3.17.1.1 | The Respondent shall provide a requirement-by-requirement compliance matrix when awarded mapping the solution to NENA 54-750. |
| 5.3.17.1.2 | The Respondent shall identify and explain any areas of non-compliance with NENA 54-750. |
| 5.3.17.1.3 | The HMI shall support accessibility requirements in accordance with ADA, including configurable font sizes, contrast, color usage, and alternative input/output methods. |
| 5.3.17.2 | The HMI shall maintain consistent layouts, icons, and workflows across call-handling functions to reduce operator error. |
| 5.3.17.3 | The solution shall support multi-monitor configurations commonly used in PSAP environments. |

| | |
|---|---|
| 5.3.17.4 | HMI views and controls shall be role-based and configurable for call-takers, supervisors, and administrators. |
| 5.3.17.5 | The HMI shall respond to user actions within defined latency thresholds suitable for emergency operations. |
| 5.3.17.6 | The HMI shall support training and simulation modes consistent with Sections 5.3.10, Solution Validation, and 5.3.11, Multi-Tenant Capability, without impacting live operations. |
| 5.3.17.7 | HMI errors, crashes, and degraded performance shall be logged and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |

| **5.3.18** | **Training** |
|---|---|
| 5.3.18.1 | Proposals shall include options for both train-the-trainer and end-user models with different training content for telecommunicator staff versus supervisors and administrators. |
| 5.3.18.1.1 | Training content differences between telecommunicators, supervisors, administrators, and technical staff shall be clearly defined and documented. |
| 5.3.18.2 | Operational training for call-handling and mapping features and functionality shall be provided to all telecommunicators and superusers. |
| 5.3.18.2.1 | Operational training shall include hands-on exercises using the Customer's configured workflows and call types. |
| 5.3.18.3 | Training for superusers shall also include monitoring, reporting, system health, and performance loggers. |
| 5.3.18.3.1 | Superuser training shall include troubleshooting scenarios and interpretation of metrics. |
| 5.3.18.4 | Training for superusers shall also include discrepancy reporting including data maintenance, validation, and error resolution workflows. |
| 5.3.18.5 | The Respondent shall include options for PSAP-specific training and train-the-trainer instruction for Customer training personnel. |
| 5.3.18.5.1 | Train-the-trainer instruction shall include guidance on maintaining training materials and onboarding new staff. |
| 5.3.18.6 | Training schedules shall accommodate 24/7 shifts. |
| 5.3.18.6.1 | Training schedules shall be coordinated with the Customer to minimize operational disruption. |
| 5.3.18.7 | All training materials shall be available in digital form. |
| 5.3.18.7.1 | Digital training materials shall remain available for the duration of the contract. |
| 5.3.18.8 | The Customer reserves the right to record all training sessions and make them available to staff online for refresher and new-agent training. This shall be at no additional charge to the Customer. |
| 5.3.18.8.1 | Recorded training sessions shall be provided in commonly used digital formats suitable for internal distribution. |
| 5.3.18.9 | 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). |
| 5.3.18.9.1 | Onsite training/coaching shall be coordinated to cover all operational shifts during the post-cutover period. |
| 5.3.18.10 | The Respondent shall provide when awarded a summary/syllabus and duration of each training class so that the PSAP can coordinate personnel schedules. |
| 5.3.18.10.1 | Training syllabi shall identify prerequisites and expected learning outcomes for each class. |
| 5.3.18.11 | Training materials shall include quick-reference guides for call-takers (CHE and mapping). |

| | |
|---|---|
| 5.3.18.11.1 | Quick-reference guides shall be tailored to Customer workflows and configurations. |
| 5.3.18.12 | Training for call-takers shall occur no more than one week prior to go-live (to facilitate retention of training material). |
| 5.3.18.12.1 | Refresher training shall be available if go-live is delayed beyond one week after training delivery. |
| 5.3.18.13 | The Respondent shall include a suite of training classes available when awarded, including in-person, on-demand, and online options. |
| 5.3.18.13.1 | The Respondent shall clearly define each training class offered, including target audience, delivery method (in-person or online), duration, and prerequisites. |
| 5.3.18.13.2 | The Respondent shall identify which training classes are included as part of system implementation and which are optional or fee-based. |
| 5.3.18.14 | The Respondent shall provide manufacturer-sponsored Customer technician certification training, where available, for a minimum of two (2) Customer personnel. Training shall be conducted in at least two (2) separate sessions held on different days. |
| 5.3.18.14.1 | Technician certification training shall include system installation, configuration, troubleshooting, recovery, and maintenance procedures, where available. |
| 5.3.18.14.2 | Certification training shall include defined completion criteria and documentation of successful completion, where available. |
| 5.3.18.15 | Customer technician training shall include refresher (or new technician) training every two years for the same number of personnel, where available. |
| 5.3.18.15.1 | Refresher training shall include updates related to system enhancements and changes since prior training. |
| 5.3.18.16 | The Respondent shall provide FE Administrator Certification training. |
| 5.3.18.16.1 | FE Administrator training shall include user management, security configuration, and system audit capabilities. |
| 5.3.18.17 | The Respondent shall provide updated training materials related to enhancements and new features after go-live. |
| 5.3.18.17.1 | Updated training materials shall be provided prior to or concurrent with the deployment of enhancements or new features. |
| 5.3.18.18 | The Respondent shall provide up-to-date online training tools after go-live. |
| 5.3.18.18.1 | Online training tools shall be updated to reflect system enhancements and configuration changes. |
| 5.3.18.19 | The Respondent shall support methods for evaluating training effectiveness, such as knowledge checks or feedback mechanisms. |
| 5.3.18.20 | The Respondent shall provide documentation or reports identifying completed training sessions and attendance, upon request. |
| 5.3.18.21 | Training delivery and materials shall be reviewed and accepted by the Customer prior to training and system cutover. |
| 5.3.18.22 | Upon request from the Customer, a train-the-trainer session on how to update, maintain, and program the FE solution shall be provided. |

| **5.3.19** | **Project Management and Progress Reports** |
|---|---|
| 5.3.19.1 | Prior to contracting with the Customer for FEs, the Respondent shall provide a high-level project plan illustrating the project timeline beginning at contract signing, the Respondent's resources and their associated roles, responsibilities, and resumes (the Customer reserves the right to refuse resources), and the expectations from the Customer. |
| 5.3.19.1.1 | The high-level project plan shall identify key milestones, dependencies, and deliverables. |

| | |
|---|---|
| 5.3.19.1.2 | Proposed project resources shall remain assigned for the duration of the project unless otherwise approved by the Customer. |
| 5.3.19.2 | The Respondent shall provide a certified project manager to lead the implementation of the Respondent's solution. |
| 5.3.19.2.1 | The certified project manager shall have prior experience implementing NG9-1-1 or FE solutions of similar size and complexity. |
| 5.3.19.3 | The Customer may request a change in project manager in the event of poor performance or lack of responsiveness. The Respondent shall execute the change within thirty (30) calendar days, if requested. |
| 5.3.19.3.1 | A replacement project manager shall possess qualifications and experience equal to or greater than the original project manager. |
| 5.3.19.4 | At a minimum, the project plan shall include the following: |
| 5.3.19.4.1 | a. Data gathering. |
| 5.3.19.4.2 | b. PSAP onsite testing. |
| 5.3.19.4.3 | c. Core component installation and testing. |
| 5.3.19.4.4 | d. FE workstation installation with third parties where applicable. |
| 5.3.19.4.5 | e. Gateway/network interface testing at all PSAP locations. |
| 5.3.19.4.6 | f. Location format, update, and discrepancy reporting mechanisms, and interface testing. |
| 5.3.19.4.7 | g. The Respondent shall identify remediation steps for any data that does not meet the minimum 98% match rate prior to acceptance. |
| 5.3.19.4.8 | h. Third-party vendor testing. |
| 5.3.19.4.9 | i. Comprehensive test and acceptance plan for all network connections verifying complete functionality with the CHE solution. |
| 5.3.19.4.10 | j. Overview of the approach and typical steps taken to ensure continuity of PSAP operations throughout the project. |
| 5.3.19.4.11 | k. Continuity plans shall be reviewed and approved by the Customer prior to execution. |
| 5.3.19.4.12 | l. Respondent's assigned Project Manager shall provide a Gantt chart project plan. |
| 5.3.19.4.13 | m. The Gantt chart shall be updated throughout the project lifecycle to reflect actual progress and approved changes. |
| 5.3.19.4.14 | n. Risks, mitigation strategies, and escalation paths related to each major project phase. |
| 5.3.19.5 | Within thirty (30) days of contract signing, the Respondent shall provide a detailed project plan, timeline, and schedule, to the contracting PSAP/agency and to the Customer if different. This plan shall include the specific approach and steps to be taken to ensure continuity of PSAP operations throughout the project. |
| 5.3.19.5.1 | Updates to the detailed project plan shall require Customer review and approval. |
| 5.3.19.6 | The Respondent shall facilitate biweekly project calls, followed by a written progress report, distributed within 24 hours of the call, capturing the minutes and action item updates from the prior project call. Calls will transition to weekly during acceptance testing and cutover planning. |
| 5.3.19.6.1 | Progress reports shall include schedule status, risks/issues, mitigation actions, and updated milestones. |
| 5.3.19.6.2 | Action items shall include assigned owners and target completion dates. |
| 5.3.19.7 | Customer billing shall be accurate and in accordance with the agreed-upon schedule and include a process for resolution of billing disputes. |
| 5.3.19.7.1 | The Respondent shall maintain a documented billing dispute resolution process and resolve billing disputes within Customer-defined timeframes. |
| 5.3.19.8 | The Respondent shall document and follow a formal change management process for scope, schedule, and cost changes, subject to Customer approval. |

| | |
|---|---|
| 5.3.19.9 | The Respondent shall maintain a project issue and risk register, updated weekly and shared with the Customer. |
| 5.3.19.10 | The Respondent shall support a formal readiness review prior to acceptance testing and cutover, including confirmation that all prerequisites have been met. |

| **5.3.20** | **Systems Integration** |
|---|---|
| 5.3.20.1 | The Respondent shall coordinate and work with the appropriate vendors' technicians for the testing and turn-up of third-party integrations (e.g., cloud vendors, CAD, logging recorder, mapping, radio, and local PSAP telephone system interfaces), as needed. |
| 5.3.20.1.1 | The Respondent shall be the primary point of coordination and accountability for all third-party system integration activities. |
| 5.3.20.1.2 | Integration test results shall be documented and provided to the Customer prior to acceptance. |
| 5.3.20.2 | The Respondent shall coordinate and work with the Customer's ESInet/NGCS vendor for system integration and testing. The Respondent's CHE solution shall support interconnection with the Customer's ESInet/NGCS, once available, at no additional cost. |
| 5.3.20.2.1 | ESInet/NGCS integration testing shall include call routing, transfer, failover, and location delivery validation. |
| 5.3.20.2.2 | Integration issues identified during testing shall be resolved prior to acceptance. |
| 5.3.20.3 | The Respondent shall support API-based integration, at no additional cost, with RapidSOS, RapidDeploy, What3Words, Prepared911, Hyper, Rave, telematics systems, real-time crime centers, and the radio log module of the Offender Data Information System (ODIS). These integrations shall be included in the base solution and shall not require separate licensing, development fees, or per-integration charges. |
| 5.3.20.3.1 | The Respondent shall support integration with future third-party data, intelligence, and public safety platforms implemented by the Customer during the contract term, through documented and supported interfaces, at no additional cost beyond the base solution. |
| 5.3.20.3.2 | Integrated third-party applications shall operate within the FE user interface without requiring a separate monitor or obstructing call-handling functionality. |
| 5.3.20.3.3 | Integrated applications shall support keyboard shortcuts and hotkey usage consistent with the CHE interface. |
| 5.3.20.3.4 | The Respondent shall clearly identify integration availability, limitations, and dependencies in its proposal. |
| 5.3.20.4 | The Respondent shall support formal integration testing and acceptance for all integrated systems prior to go-live. |
| 5.3.20.5 | The Respondent shall provide documentation for all supported system interfaces, including data flows, protocols, and dependencies. |
| 5.3.20.6 | Changes to integrated systems or interfaces shall follow a documented change management process and be approved by the Customer. |

| **5.3.21** | **Change Management** |
|---|---|
| 5.3.21.1 | The Respondent shall maintain a documented change-management process that adheres to the Information Technology Infrastructure Library (ITIL) Change Management framework for Standard, Emergency, and Normal changes (Major, Significant, and Minor). |
| 5.3.21.1.1 | The change-management process shall be documented and provided to the Customer for review and acceptance prior to go-live. |

| | |
|---|---|
| 5.3.21.1.2 | The process shall apply to all changes that could impact CHE availability, performance, security, or functionality. |
| 5.3.21.2 | The Respondent shall use an ITIL-aligned Request for Change (RFC) process for planned changes, submitted to the Customer at least seventy-two (72) hours prior to scheduled maintenance. |
| 5.3.21.2.1 | Each RFC shall include, at a minimum:<br>a. A clear and concise description of the proposed change<br>b. Reason for the change<br>c. Scope of the change<br>d. Potential impacts and risks<br>e. Expected benefits<br>f. Dependencies and relationships<br>g. Implementation change management plan<br>h. Backout plan<br>i. Authorization and Approval |
| 5.3.21.2.2 | Emergency changes shall be documented and submitted to the Customer within five (5) calendar days of implementation. |
| 5.3.21.2.3 | RFCs shall clearly identify whether the change is classified as Standard, Emergency, or Normal (Major, Significant, or Minor). |
| 5.3.21.3 | The Respondent shall provide a documented process by which the Customer may request changes. |
| 5.3.21.3.1 | Customer-initiated change requests shall be tracked, prioritized, and reported using the same ITSM process as Respondent-initiated changes. |
| 5.3.21.3.2 | The Respondent shall provide visibility into the status of Customer-initiated changes. |
| 5.3.21.4 | The Respondent shall support automated ITIL-aligned change status notifications through an ITSM platform. |
| 5.3.21.4.1 | Change notifications shall be triggered at defined lifecycle points, including RFC creation, review, approval, scheduling, execution, and post-change review. |
| 5.3.21.4.2 | The ITSM platform shall be configurable by the Customer to define notification timing, content, and recipients. |
| 5.3.21.5 | The Respondent shall define and follow procedures for complete backup of all impacted systems and data immediately prior to change implementation, including use of a 3-2-1 backup strategy. |
| 5.3.21.5.1 | Backup completion shall be verified and documented prior to implementing the change. |
| 5.3.21.5.2 | Backup integrity shall be tested monthly tested to ensure successful restoration. |
| 5.3.21.6 | The Respondent shall include the ability for the Customer to initiate a rollback request. |
| 5.3.21.6.1 | Rollback procedures shall be documented, tested, and available to Customer personnel. |
| 5.3.21.6.2 | Rollback execution and outcomes shall be logged and reported to the Customer. |
| 5.3.21.7 | Each change shall include an explicit impact assessment covering service availability, performance, security, interoperability, and compliance. |
| 5.3.21.8 | The Respondent shall support Customer-defined maintenance windows and blackout periods during which non-emergency changes are prohibited. |
| 5.3.21.9 | The Respondent shall provide periodic reports summarizing implemented changes, failed changes, rollbacks, and emergency changes. |

| **5.3.22** | **Change Orders** |
|---|---|
| 5.3.22.1 | The Respondent shall submit all change orders in writing. |
| 5.3.22.1.1 | Written change orders shall include a unique identifier and revision history. |

| | |
|---|---|
| 5.3.22.2 | All change orders shall require prior written approval by the Customer before any associated work is performed, regardless of whether the change relates to equipment, services, scope, schedule, or other contractual elements. |
| 5.3.22.2.1 | Approved change orders shall clearly identify scope, schedule impact, and cost impact, if any. |
| 5.3.22.2.2 | No work associated with a change order shall begin until written approval is received from the Customer. |
| 5.3.22.3 | The Customer shall not accept change orders resulting in additional costs unless additional features are requested by the Customer. |
| 5.3.22.3.1 | Any proposed change order that does not result in additional cost shall still require Customer approval. |
| 5.3.22.3.2 | Change orders shall not be used to remediate deficiencies, defects, or non-compliance with contractual requirements identified during testing, acceptance, or operations. |
| 5.3.22.4 | Each change order shall include a detailed description of the change, justification, impact analysis (scope, schedule, cost), and dependencies. |
| 5.3.22.5 | The Respondent shall maintain a log of all submitted, approved, rejected, and completed change orders and make it available to the Customer upon request. |
| 5.3.22.6 | Emergency change orders shall be documented and submitted for Customer review and ratification Within 24hoursfollowing implementation. |

| **5.3.23** | **Service Interruptions and Facility Damages** |
|---|---|
| 5.3.23.1 | During installation and cutover, the Respondent shall ensure that the PSAP experiences minimal interruption to normal business operations. |
| 5.3.23.1.1 | Installation and cutover activities shall be planned and executed to avoid disruption to live 9-1-1 operations whenever possible. |
| 5.3.23.1.2 | Any anticipated service interruption shall be communicated to the Customer in advance and approved prior to execution. |
| 5.3.23.2 | Prior to any PSAP visit, the Respondent shall provide advance notice to, and obtain authorization from, the Customer, who reserves the right to alter or suspend the intended schedule for any reason at its sole discretion. |
| 5.3.23.2.1 | Advance notice shall include the scope of work (SOW), personnel involved, expected duration, and potential operational impacts. |
| 5.3.23.2.2 | All Respondent and subcontractor personnel shall comply with Customer facility access, security, and identification requirements. |
| 5.3.23.3 | The Respondent shall be responsible for the repair and/or restoration of any damages or outages caused by the Respondent, its subcontractors, or delivery personnel to any PSAP or agency facilities through the receipt, delivery, installation, or testing of the solution. |
| 5.3.23.3.1 | Repairs or restoration shall be completed at no cost to the Customer. |
| 5.3.23.3.2 | Restoration shall return affected facilities and services to their original or better condition. |
| 5.3.23.3.3 | Damages or outages shall be reported to the Customer immediately upon discovery, along with a remediation plan and timeline. |
| 5.3.23.4 | The Respondent shall document any service interruption or facility damage, including root cause, corrective actions taken, and preventive measures to avoid recurrence. |
| 5.3.23.5 | The Respondent shall maintain adequate insurance coverage to address potential damages or outages caused during installation, testing, or cutover activities, and shall provide proof of coverage upon request. |
| 5.3.23.6 | The Respondent shall be fully responsible for the actions and performance of all subcontractors and delivery personnel involved in the project. |

| 5.3.24 | Storage, Staging, Delivery, and Inventory Control |
|---|---|
| 5.3.24.1 | The Respondent shall be accountable for the storage of materials until such time that the items are to be installed. |
| 5.3.24.1.1 | Stored equipment shall be maintained in secure, environmentally appropriate facilities consistent with manufacturer specifications. |
| 5.3.24.2 | No Customer facilities, including PSAPs, may be used as a warehouse for uninstalled equipment. |
| 5.3.24.3 | The Respondent shall coordinate with the Customer for the shipping, staging, and testing of all equipment prior to installation. |
| 5.3.24.3.1 | Shipping and staging schedules shall be approved by the Customer prior to execution. |
| 5.3.24.4 | The Respondent shall be responsible for ensuring that the equipment is fully staged, configured, and tested prior to delivery to the Customer. |
| 5.3.24.4.1 | Pre-delivery testing shall include verification against Customer-approved configurations. |
| 5.3.24.4.2 | Test results shall be documented and provided to the Customer upon request. |
| 5.3.24.5 | The Respondent shall arrange for equipment to be delivered onsite as needed in accordance with the approved installation schedule. The cost of delivery shall be included in the Respondent's proposal. |
| 5.3.24.6 | The Respondent shall be responsible for the receipt, inventory, and movement of all materials. |
| 5.3.24.6.1 | Inventory records shall be updated in near-real time as materials are received, moved, or installed. |
| 5.3.24.7 | The Respondent shall be responsible for the disposal of shipping material, as well as the daily removal of other refuse. |
| 5.3.24.7.1 | Disposal activities shall comply with Customer facility rules and applicable environmental regulations. |
| 5.3.24.8 | The Respondent shall provide the Customer with a detailed inventory of all equipment installed on PSAP premises. |
| 5.3.24.8.1 | Equipment inventories shall be provided to the Customer prior to acceptance testing and updated upon final acceptance. |
| 5.3.24.9 | At a minimum, the inventory data shall include where equipment is installed, the manufacturer, part number, serial number, quantity, and model number. |
| 5.3.24.10 | The Respondent shall provide the equipment inventory in hard- and soft-copy format using Microsoft Excel. |
| 5.3.24.10.1 | Electronic inventory files shall be editable and not password protected. |
| 5.3.24.11 | The Respondent shall be responsible for all hardware, from its receipt prior to staging until it is accepted by the Customer in writing. |
| 5.3.24.11.1 | Written acceptance shall be defined by the Customer and may include partial or phased acceptance. |
| 5.3.24.12 | Any hardware or equipment lost, misplaced, or damaged prior to acceptance shall be replaced at the Respondent's sole expense. |
| 5.3.24.13 | Designated Customer technicians shall participate in the deployment of positions at PSAP facilities. During equipment installation, the Respondent shall coordinate with Customer staff and allow any asset tagging and/or labeling to occur, as deemed appropriate by Customer staff. |
| 5.3.24.13.1 | Installation schedules shall allow sufficient time for Customer asset tagging and verification activities. |
| 5.3.24.14 | The Respondent shall support inventory reconciliation with Customer personnel prior to system acceptance. |

| | |
|---|---|
| 5.3.24.15 | The Respondent shall provide configuration baseline documentation linking installed equipment to the approved system design. |
| 5.3.24.16 | If applicable, the Respondent shall coordinate the removal and disposition of replaced or legacy equipment in accordance with Customer direction. |

| **5.3.25** | **Code Compliance, Grounding, and Transient Voltage Surge Suppression** |
|---|---|
| 5.3.25.1 | Installation shall comply with all applicable national, state, and local codes. |
| 5.3.25.1.1 | Code compliance shall include, at a minimum, applicable electrical, fire, building, grounding, and life-safety codes. |
| 5.3.25.1.2 | The Respondent shall correct, at no cost to the Customer, any non-compliant Respondent installation identified during inspection or acceptance testing. |
| 5.3.25.2 | All metallic data or voice circuits shall be equipped with both primary and secondary transient voltage surge suppression (TVSS) devices per industry standards for telecommunications equipment. |
| 5.3.25.2.1 | TVSS devices shall be installed in accordance with manufacturer specifications and applicable codes. |
| 5.3.25.2.2 | TVSS protection shall not degrade signal quality or system performance. |
| 5.3.25.3 | 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. |
| 5.3.25.3.1 | Operational indicators shall be clearly visible or audible to maintenance personnel during normal operations. |
| 5.3.25.3.2 | Failed or exercised TVSS devices shall be replaced within Customer-defined service level timeframes. |
| 5.3.25.4 | Each PSAP where TVSS devices are installed shall be provided with an onsite spares kit to assist in emergency restoration. |
| 5.3.25.4.1 | The spares kit shall include sufficient quantities to restore protection for all protected circuits at the PSAP. |
| 5.3.25.4.2 | Spares inventory shall be documented and replenished by the Respondent as components are used. |
| 5.3.25.5 | TVSS equipment shall comply with UL 497A, *Secondary Protectors for Communications Circuits*. |
| 5.3.25.6 | The Respondent shall provide all necessary equipment, interfaces, and cables to ensure power requirements (voltage, wattage) for the proposed equipment (e.g., FE and backroom equipment). |
| 5.3.25.6.1 | Power requirements for all proposed FE and backroom equipment shall be documented and provided to the Customer prior to installation. |
| 5.3.25.6.2 | Power requirement documentation shall include normal, peak, and startup load conditions. |
| 5.3.25.6.3 | Power requirements shall identify compatibility with existing PSAP power and uninterruptible power supply (UPS) systems. |
| 5.3.25.7 | The Respondent shall ensure all equipment is properly grounded and bonded in accordance with applicable codes and telecommunications grounding standards. |
| 5.3.25.8 | The Respondent shall support inspection and verification of code compliance and grounding prior to system acceptance. |
| 5.3.25.9 | As-built documentation shall identify installed TVSS devices, grounding points, and power connections. |

| **5.3.26** | **Pre-Cutover Acceptance Criteria** |
|---|---|
| 5.3.26.1 | The Respondent shall provide evidence of redundant backups in at least two geo-diverse locations of all configuration files and databases for all customer-premise-installed equipment. |

| | |
|---|---|
| 5.3.26.1.1 | Backup frequency and retention periods shall be documented and approved by the Customer. |
| 5.3.26.1.2 | Backup restoration procedures shall be tested and results documented prior to cutover. |
| 5.3.26.2 | The Respondent shall provide confirmation and documentation of system control, monitoring, and alarm solutions. |
| 5.3.26.2.1 | Documentation shall clearly identify system control, monitoring, and alarm components and their operational status. |
| 5.3.26.3 | The Respondent shall provide an inventory of all Respondent-provided, Customer premise-installed equipment, including manufacturer, model, part number, quantity, serial number, and installed location. |
| 5.3.26.3.1 | Inventory shall reflect final installed configurations and be validated by the Customer prior to acceptance. |
| 5.3.26.4 | The Respondent shall provide acceptance test plan documentation to be reviewed and approved by the Customer. |
| 5.3.26.4.1 | The acceptance test plan shall demonstrate traceability to all applicable contractual requirements. |
| 5.3.26.4.2 | Acceptance test results shall be documented and provided to the Customer. |
| 5.3.26.5 | During testing, if Customer staff believes that a solution test fails, the Customer will provide the Respondent with a written description of what test failed and why. The Respondent shall work expeditiously to resolve the problem and provide an estimated resolution time to the Customer. |
| 5.3.26.5.1 | Corrective actions and retesting results shall be documented and submitted to the Customer for review. |
| 5.3.26.5.2 | Repeated test failures shall trigger formal escalation and potential corrective action in accordance with, Escalation Procedures. |
| 5.3.26.6 | The Respondent shall provide final as-built drawings (in editable Visio, Lucid chart, or draw.io format), system-wide and on an individual PSAP basis, within thirty (30) days of cutover. |
| 5.3.26.6.1 | As-built drawings shall reflect the final, accepted configuration at cutover. |
| 5.3.26.7 | As-built document shall be provided in a read-only format with an additional, editable copy for customer to use as the system evolves. As-built documentation shall include all customer-premise-installed cabling, equipment, and configurations, bringing attention to unique or special deployment details, as well as IP addresses and hostnames for network information and model numbers, serial numbers, and warranty dates for equipment. |
| 5.3.26.7.1 | As-built documentation shall be reviewed and accepted by the Customer as a prerequisite to final acceptance. |
| 5.3.26.8 | The Respondent shall provide a checklist when awarded that includes all items identified in this RFP response and any resulting contract. This checklist will be evaluated prior to go-live. |
| 5.3.26.8.1 | All checklist items shall be verified and signed off by the Customer prior to go-live. |
| 5.3.26.8.2 | Exceptions or open items shall require written Customer approval prior to cutover. |
| 5.3.26.9 | The Customer shall retain sole authority to determine go/no-go readiness for cutover based on acceptance results. |
| 5.3.26.10 | The Respondent shall support a formal cutover readiness review prior to go-live, including confirmation that all pre-cutover criteria have been met. |
| 5.3.26.11 | Final acceptance shall require written sign-off by the Customer. |

| 5.3.27 | Cutover Coordination |
|---|---|
| 5.3.27.1 | The Respondent shall coordinate cutover activities with all service providers and Customer personnel. |
| 5.3.27.1.1 | The Respondent shall serve as the single point of coordination and accountability for all cutover activities. |
| 5.3.27.2 | A detailed cutover plan, along with coordination conference calls and supporting documentation, shall be provided to the Customer and all participating parties at least forty-five (45) calendar days prior to the scheduled cutover date. |
| 5.3.27.2.1 | The detailed cutover plan shall include roles, responsibilities, timelines, dependencies, risks, and rollback procedures. |
| 5.3.27.2.2 | The cutover plan shall identify decision points and escalation paths during cutover. |
| 5.3.27.3 | The Respondent shall review the final cutover plan with Customer staff at least fourteen (14) days prior to cutover. |
| 5.3.27.3.1 | Any changes to the cutover plan after the fourteen (14)-day review shall require Customer approval. |
| 5.3.27.4 | The Respondent shall provide trained and capable technical and functional solution support, and the project manager and technical personnel shall be available and onsite the day of cutover. |
| 5.3.27.4.1 | Onsite personnel shall be authorized to make immediate decisions required to support cutover success. |
| 5.3.27.5 | 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. |
| 5.3.27.5.1 | Onsite end-user support shall be coordinated to cover all active operational shifts during cutover. |
| 5.3.27.6 | The Respondent shall provide onsite technical support staff dedicated to issue resolution, troubleshooting, and system stabilization for each cutover. |
| 5.3.27.6.1 | The Respondent shall commit to a defined duration of onsite technical support for each cutover. |
| 5.3.27.6.2 | Any reduction in onsite support duration shall require Customer approval. |
| 5.3.27.7 | The Respondent shall confirm in writing that all pre-cutover acceptance criteria in Section 5.3.26, Pre-Cutover Acceptance Criteria, have been met prior to cutover. |
| 5.3.27.8 | The Respondent shall provide real-time status updates during cutover, including issue tracking and escalation status, and shall deliver a post-cutover report after each cut if multiple are involved, summarizing outcomes, issues, resolutions, and follow-up actions. |
| 5.3.27.9 | The Customer shall retain the authority to pause or rollback cutover activities if unacceptable operational risk is identified. |

| 5.3.28 | Call-Handling Acceptance Testing |
|---|---|
| 5.3.28.1 | The Customer's call-handling acceptance testing is intended to validate that the Respondent's solution functions as expected in the PSAP environment and as asserted in its 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 thirty (30) days prior to PSAP cutover and must not have any Priority 1 or Priority 2 faults for the PSAP cutover(s) to occur. |
| 5.3.28.1.1 | Acceptance testing shall include validation of normal operations, failover, recovery, and degraded mode scenarios. |
| 5.3.28.1.2 | Acceptance testing shall be conducted using the final production configuration. |

| | |
|---|---|
| 5.3.28.2 | The selected Respondent shall provide a baseline call-handling acceptance test plan (including specific test cases, scenarios, and expected outcomes) to the Customer at least thirty (30) days in advance of the planned execution thereof and allow the Customer a full two (2) weeks to modify the test plan to meet its system acceptance criteria. |
| 5.3.28.2.1 | Test cases shall demonstrate traceability to all applicable contractual requirements. |
| 5.3.28.2.2 | Test execution results shall be documented and provided to the Customer. |
| 5.3.28.3 | If a failure occurs, the Customer will provide a written notification to the Respondent with its classification of the fault according to the following four categories:<br>a. Priority 1 Fault — A critical system fault that renders the solution fully or partially inoperable. These faults are unacceptable to the Customer.<br>b. Priority 2 Fault — A major system fault that significantly reduces the solution's performance and ability to function. These faults are unacceptable to the Customer and must be resolved before the Customer will accept the solution.<br>c. Priority 3 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 the Customer will accept the final solution.<br>d. Priority 4 Fault — A combination of minor system faults and items that are on a punch list or product roadmap. These items shall have minimal or no effect on system performance and shall either be resolved prior to final acceptance or have a Customer-approved remediation timeline documented in writing. |
| 5.3.28.3.1 | All identified faults shall be logged, tracked, and reported with status updates until resolution. |
| 5.3.28.4 | If the Respondent disputes the Customer's fault classification, a call will be held at the earliest possible opportunity to resolve the disagreement. Parties to that call shall include Customer personnel, the Respondent, and, at the Customer's discretion, representative(s) from the PSAP. If agreement is not reached within thirty (30) minutes, the Customer's classification will prevail. |
| 5.3.28.4.1 | The Respondent shall document the outcomes of fault classification discussions and retain them as part of acceptance records. |
| 5.3.28.5 | The Respondent shall remedy non-compliance per the Service Levels and Service Management Performance Standard sections of any resulting contract and shall provide written notification of the remedy to the Customer. |
| 5.3.28.5.1 | Remediation actions shall include timelines for correction and retesting. |
| 5.3.28.6 | If a Priority 1 or Priority 2 fault occurs during acceptance testing, the Respondent shall remediate the fault and repeat the acceptance test. Cutover shall not proceed until no Priority 1 or Priority 2 faults remain. |
| 5.3.28.6.1 | Retesting shall include all impacted test cases and related functional areas. |
| 5.3.28.7 | The Respondent shall confirm in writing that all pre-cutover acceptance criteria in Section 5.3.26, Pre-Cutover Acceptance Criteria, have been met prior to cutover. |
| 5.3.28.7.1 | The Customer shall provide written confirmation of acceptance testing completion prior to cutover. |
| 5.3.28.8 | The Respondent shall ensure that no system, configuration, or software changes are made during acceptance testing without prior written Customer approval. |
| 5.3.28.9 | The Customer and PSAP personnel shall have the right to witness and participate in acceptance testing. |
| 5.3.28.10 | Acceptance test plans, results, and defect logs shall be retained in accordance with Customer evidentiary and audit requirements. |

| 5.3.29 | FE Acceptance Testing |
|---|---|
| 5.3.29.1 | The Customer's FE acceptance testing is intended to validate overall system performance, especially system-level functionality not otherwise verifiable during individual PSAP acceptance testing and includes, at a minimum, testing of the following:<br>a. Inter-PSAP transfers and conferences.<br>b. Automatic system failover and maintenance of full system functionality when a redundant element is taken out of service.<br>c. Alternate routing under functional element and network component failure scenarios.<br>d. High call volume performance. |
| 5.3.29.1.1 | System acceptance testing shall validate system-wide behavior across all PSAPs operating as part of the solution. |
| 5.3.29.2 | System acceptance testing shall be conducted using the final production configuration across all participating PSAPs. |
| 5.3.29.3 | The Respondent shall provide a baseline System Acceptance Test Plan (including specific test cases, scenarios, and expected outcomes) to the Customer at least thirty (30) days in advance of the planned execution thereof and allow the contracting PSAP(s) a full two (2) weeks to modify the test plan to reflect its system acceptance criteria. |
| 5.3.29.3.1 | System acceptance test cases shall demonstrate traceability to all applicable contractual requirements. |
| 5.3.29.3.2 | Test execution results shall be documented and provided to the Customer. |
| 5.3.29.4 | If a failure occurs: |
| 5.3.29.4.1 | The Customer will provide a written notification to the Respondent with its classification of the fault according to the four categories identified in Section 5.3.28.3 of this document. |
| 5.3.29.4.2 | If the Respondent disputes the Customer's fault classification, a call will be held at the earliest possible opportunity to resolve the disagreement. Parties to that call shall include Customer personnel, the Respondent, and at the Customer's discretion, representative(s) from the PSAP. If agreement is not reached within thirty (30) minutes, the Customer's classification will prevail. |
| 5.3.29.4.3 | The Respondent shall remedy non-compliance per the Service Levels and Service Management Performance Standard sections of any resulting contract and shall provide written notification of the remedy to the Customer. |
| 5.3.29.4.4 | The system acceptance testing process shall continue until all test cases are executed without Priority 1 and Priority 2 faults, at which point the system shall be deemed eligible for PSAP cutover activities in accordance with Section 5.3.27, Cutover Coordination. |
| 5.3.29.4.5 | All system acceptance test failures shall be logged, tracked, and reported with status updates until resolution. |
| 5.3.29.4.6 | The Customer shall provide written confirmation of system acceptance testing completion prior to proceeding with cutover. |
| 5.3.29.5 | No system, configuration, or software changes shall be implemented during system acceptance testing without prior written Customer approval. |
| 5.3.29.6 | The Customer and PSAP personnel shall have the right to participate in and witness system acceptance testing. |
| 5.3.29.7 | System acceptance test plans, results, and defect logs shall be retained in accordance with Customer evidentiary and audit requirements. |

| 5.3.30 | Transition Plan |
|---|---|
| 5.3.30.1 | Within 30 days of contract signing, the Respondent shall provide a detailed transition plan that includes a full description of the methods and procedures to be employed to ensure a non-service-affecting transition from the current call-handling environment to the new system. The transition plan shall align with the acceptance and cutover requirements defined in Sections 5.3.26-5.3.28 and shall not permit transition activities to begin prior to Customer acceptance. |
| 5.3.30.1.1 | The transition plan shall identify key milestones, dependencies, risks, and mitigation strategies. |
| 5.3.30.1.2 | The transition plan shall be reviewed and approved by the Customer prior to execution. |
| 5.3.30.2 | The Respondent shall provide transition recommendations considering the complexity of the specific deployment environment. |
| 5.3.30.2.1 | The transition plan shall account for site-specific operational, technical, and staffing constraints identified by the Customer. |
| 5.3.30.3 | 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 the Customer's configuration. |
| 5.3.30.3.1 | The proposed migration order and durations shall be coordinated with and approved by the Customer. |
| 5.3.30.3.2 | Any changes to the approved migration sequence shall require Customer approval. |
| 5.3.30.4 | The migration plan shall include a fallback procedure to restore the PSAP to a pre-transition operational state in the event of a severe failure. |
| 5.3.30.4.1 | Fallback procedures shall be tested or validated prior to transition execution. |
| 5.3.30.4.2 | Authority to initiate fallback shall rest solely with the Customer and may be exercised at the Customer's discretion. |
| 5.3.30.5 | The Respondent shall provide a communication plan identifying notifications, stakeholders, escalation paths, and status reporting during transition activities. |
| 5.3.30.6 | Prior to each agency or site transition, the Respondent shall confirm readiness criteria have been met and obtain Customer approval to proceed. |
| 5.3.30.7 | The Respondent shall support post-transition validation to confirm full functionality, performance, and stability following migration, with documented results provided to the Customer. |

| 5.3.31 | Software Release Management |
|---|---|
| 5.3.31.1 | The Respondent shall provide a schedule of software releases and shall document the decision-making processes used to determine which features and defect resolutions are included, deferred, or excluded from each scheduled release. |
| 5.3.31.1.1 | Scheduled software releases shall be classified (e.g., major, minor, maintenance, emergency) with defined characteristics. |
| 5.3.31.1.2 | The Customer shall be notified of planned release scope and impacts prior to scheduling. |
| 5.3.31.2 | Maintenance releases and feature releases shall be provided to all Customers at no cost while a maintenance agreement is in place. |
| 5.3.31.2.1 | No-cost release coverage shall include all Respondent-controlled and required third-party software components. |
| 5.3.31.3 | The Respondent shall provide defect-resolution software releases, and the decision-making processes involved in selecting which software defects to resolve. |
| 5.3.31.3.1 | Defect-resolution release prioritization shall consider defect severity, operational impact, and SLA risk. |

| | |
|---|---|
| 5.3.31.3.2 | Critical defect resolutions shall not be deferred to future releases without Customer approval. |
| 5.3.31.4 | The Respondent shall notify and coordinate scheduling with the Customer whenever solution servicing requires onsite visits. Notification shall occur no less than ten (10) business days before the needed visit, and scheduling shall be at the sole discretion of the Customer. |
| 5.3.31.4.1 | Onsite servicing activities shall be clearly identified by scope and expected impact. |
| 5.3.31.4.2 | Emergency servicing actions shall be documented and communicated to the Customer as soon as practicable. |
| 5.3.31.5 | The Respondent shall include in its proposal the procedure for managing and tracking 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 Customer staff. |
| 5.3.31.5.1 | Configuration management procedures shall align with the change management process defined in Section 5.3.21, Change Management. |
| 5.3.31.5.2 | Configuration changes shall be logged and auditable. |
| 5.3.31.6 | The Respondent shall provide release notes to the Customer no less than ten (10) business days prior to system upgrades or updates, clearly identifying any new functionality of which the Customer may wish to take advantage. |
| 5.3.31.6.1 | Release notes shall identify new, modified, deprecated, or removed functionality. |
| 5.3.31.6.2 | Release notes shall identify known issues and mitigations. |
| 5.3.31.7 | The Respondent shall request authorization from the Customer no less than ten (10) 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. Such authorization shall follow the change-management requirements defined in Section 5.3.21, Change Management. |
| 5.3.31.7.1 | Emergency changes shall be documented and reviewed with the Customer following implementation. |
| 5.3.31.7.2 | Emergency changes shall be limited to actions necessary to restore service. |
| 5.3.31.8 | The Respondent shall support testing of and integration of any third-party software upon which the solution is built. This includes, but is not limited to, operating systems, libraries, programming or scripting language interpreters or compilers, utilities, and applications. |
| 5.3.31.8.1 | Third-party software integration testing shall be performed on a defined schedule and prior to production deployment. |
| 5.3.31.8.2 | The Customer shall be notified of third-party software changes that may impact the solution. |
| 5.3.31.9 | The licensing and maintenance costs of third-party software, as defined in Section 5.3.31.8 above, shall be included in the cost of the Respondent's solution. |
| 5.3.31.9.1 | The Respondent shall disclose all third-party software components included in the solution. |
| 5.3.31.9.2 | No additional licensing, maintenance, or integration fees for required third-party software components shall be charged to the Customer during the contract term. |
| 5.3.31.10 | The Respondent shall integrate defect-resolution software releases, and the decision-making processes involved in selecting which defect-resolution software releases to integrate (as opposed to those skipped). |
| 5.3.31.10.1 | Decisions to defer or skip defect-resolution releases shall be documented and communicated to the Customer. |

| | |
|---|---|
| 5.3.31.10.2 | The Customer shall be notified when defect-resolution releases addressing service-impacting issues are not integrated. |

| **5.3.32** | **Warranty and Monitoring** |
|---|---|
| 5.3.32.1 | For all software and Respondent-provided hardware, the Respondent shall include 24/7/365 parts and labor warranty for the duration of the contract, defined as ten (10) years from the date of final Customer acceptance. The Respondent shall provide 24/7/365 extended warranty (parts and labor) for optional two (2)-year extensions. |
| 5.3.32.1.1 | Warranty coverage shall begin upon final written Customer acceptance. |
| 5.3.32.1.2 | Warranty services shall meet or exceed the response and repair timeframes defined in Appendix A. |
| 5.3.32.2 | For all software and Respondent-provided hardware, warranties shall cover hardware, cabling and connectors, and software, and include 24/7/365 phone and web support. |
| 5.3.32.2.1 | Warranty coverage shall include the firmware, security patches, and minor software updates required to maintain system operability and security. |
| 5.3.32.3 | The Respondent shall provide continuous (24/7/365) remote system monitoring and maintenance through designated monitoring facilities. |
| 5.3.32.3.1 | Remote system monitoring and maintenance shall apply to all solution components. |
| 5.3.32.3.2 | Monitoring shall include, at a minimum, queue state, element state (e.g., call-handling servers, workstations, routers, and other network devices), interfaces, and supporting infrastructure. |
| 5.3.32.3.3 | Monitoring facilities shall include primary and secondary NOC/SOC capabilities located within North America and shall support monitoring of Policy Routing Functions (PRF) in accordance with the NENA i3 standard. |
| 5.3.32.4 | The Respondent's NOC services shall include proactive and reactive maintenance plans. The response shall include details regarding the number of certified technicians who reside within a two-hour drive of each call-handling site. |
| 5.3.32.4.1 | Local technician availability commitments shall be aligned with repair time SLAs. |
| 5.3.32.4.2 | Changes to local technician coverage shall be communicated to the Customer. |
| 5.3.32.5 | System monitoring provided by the Respondent shall include a near-real-time portal through which the PSAP may configure a dashboard-type view for monitoring its data and voice activity as well as overall system status and health. |
| 5.3.32.5.1 | Portal access shall be governed by role-based access controls. |
| 5.3.32.5.2 | Portal data shall be updated in real- or near-real time. |
| 5.3.32.6 | The Respondent shall provide after awarding a process to support repair or replacement of out-of-warranty items. |
| 5.3.32.6.1 | The Respondent shall document processes and procedures for repair or replacement of out-of-warranty components. |
| 5.3.32.6.2 | Estimated costs for out-of-warranty repairs or replacements shall be disclosed in advance and require Customer approval. |
| 5.3.32.6.3 | Out-of-warranty repair services shall not degrade contracted service levels. |
| 5.3.32.7 | The Respondent shall perform preventive maintenance activities as part of the warranty and monitoring services and document such activities with logs being available upon request. |
| 5.3.32.8 | Monitoring alerts shall be classified by severity and escalated in accordance with Section 5.3.5, Monitoring and Alarming, and Appendix A. |
| 5.3.32.9 | Warranty coverage shall remain in effect in the event of PSAP consolidation or reconfiguration within the Customer environment. |

| 5.3.33 | Incident and Trouble Reporting |
|---|---|
| 5.3.33.1 | The Respondent shall implement a process to initiate, track, communicate status, and resolve trouble reports. |
| 5.3.33.1.1 | The Respondent shall maintain documented procedures for initiating, tracking, communicating status, and resolving incidents and trouble reports. |
| 5.3.33.1.2 | Incident and trouble reporting procedures shall align with the service levels and escalation requirements defined in Appendix A. |
| 5.3.33.1.3 | Trouble reports shall be tracked from initiation through resolution with status updates available to the Customer. |
| 5.3.33.1.4 | Resolution activities shall include root cause identification and corrective actions where applicable. |
| 5.3.33.1.5 | Remote monitoring, maintenance, troubleshooting, and repair capabilities shall be available on 24/7/365. |
| 5.3.33.1.6 | Use of remote access for troubleshooting shall comply with Customer security and access control policies. |
| 5.3.33.1.7 | Incident records, status changes, and resolution details shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.3.33.2 | In addition to built-in capabilities, the Respondent shall interface with other management systems using standard protocols such as SNMP or Common Management Information Protocol (CMIP) or an equivalent Customer-approved management interface. |
| 5.3.33.2.1 | Integration with external management systems shall be configurable by the Customer. |
| 5.3.33.2.2 | Events and alarms shared with external systems shall include severity, timestamp, affected components, and status. |
| 5.3.33.3 | The Respondent shall classify incidents by severity and priority consistent with Appendix A. |
| 5.3.33.4 | The Respondent shall provide automated notifications to the Customer for incident creation, status changes, escalation, and resolution. |
| 5.3.33.5 | The Respondent shall provide periodic (at least monthly) reports summarizing incident volume, response times, resolution times, and recurring issues. |

| 5.3.34 | Escalation Procedures |
|---|---|
| 5.3.34.1 | Following cutover, the Respondent shall maintain and provide documented escalation procedures for issue resolution. |
| 5.3.34.1.1 | Escalation documentation shall be provided to the Customer prior to cutover and kept current throughout the contract term. |
| 5.3.34.1.2 | Escalation contact information shall include primary and secondary contacts for each escalation tier. |
| 5.3.34.1.3 | Updates to escalation documentation shall be communicated to the Customer within a Customer-defined timeframe. |
| 5.3.34.2 | The Respondent shall notify the Customer of any specific issues, address how future occurrences will be avoided (risk mitigation), and provide a suggested path toward resolution. |
| 5.3.34.2.1 | Escalation responses shall include documented root cause analysis for service-impacting issues. |
| 5.3.34.2.2 | Risk mitigation actions shall be tracked to completion and reported to the Customer. |
| 5.3.34.3 | The escalation process shall address inclusion of the manufacturer (if other than Respondent) in meetings and discussions with affected PSAPs when the Respondent's efforts have not resolved the issue. |

| | |
|---|---|
| 5.3.34.3.1 | Manufacturer engagement shall not delay escalation timelines or resolution commitments. |
| 5.3.34.3.2 | The Customer shall be included in all escalation communications involving manufacturers. |
| 5.3.34.4 | The Respondent shall provide an escalation process and procedures regarding resolution of critical defects, including time to resolution and engagement of Tier 3 or Tier 4 engineering and development resources. |
| 5.3.34.4.1 | Escalation timelines for Tier 3 and Tier 4 engagement shall align with SLRs in Appendix A. |
| 5.3.34.4.2 | Escalation procedures shall define handoff criteria between Tier levels. |
| 5.3.34.4.3 | Critical defect escalation status shall be communicated to Customer at Customer-defined intervals. |
| 5.3.34.5 | The Customer shall have the authority to invoke escalation to higher tiers at its sole discretion when service level objectives are at risk or service quality is otherwise unacceptable. |
| 5.3.34.6 | The Respondent shall track all escalated issues and provide escalation reports including issue description, severity, actions taken, and resolution status. |
| 5.3.34.6.1 | Escalated issues and escalation actions shall be tracked within the incident management process defined in Sections 5.3.33-5.3.34. |
| 5.3.34.7 | Following resolution of a critical escalated issue, the Respondent shall conduct a post-incident review within a Customer-defined timeframe and provide documented findings, root cause analysis, corrective actions, and preventive measures to the Customer. |

| **5.3.35** | **Software Backup and Restoration** |
|---|---|
| 5.3.35.1 | If the Respondent is hosting the infrastructure (e.g., SaaS) then the Respondent shall perform automatic backups of software, as well as all PSAP-specific configurations and databases. The backups shall not materially degrade performance. If the Respondent is not hosting the infrastructure, the Respondent shall provide a documented backup and restoration plan for system components within the Respondent's scope. |
| 5.3.35.1.1 | Backups for hosted solutions shall include all application software, configuration files, system settings, and databases required to restore full operational capability. |
| 5.3.35.1.2 | Backups shall be performed in a manner that does not degrade call-handling, mapping, analytics, or interface performance. |
| 5.3.35.1.3 | If the Respondent does not host the infrastructure, the Respondent shall provide a documented backup plan (not recommendations) for all Respondent-provided and Customer-premise-installed components within the Respondent's scope. |
| 5.3.35.2 | The Respondent shall implement a Customer-approved backup schedule for the workstations, servers, and any other Customer-premise-installed devices that have databases, operating systems, or configurations that may be backed up. |
| 5.3.35.2.1 | The Respondent shall provide a backup schedule that identifies, for each system component (workstations, servers, and any Customer-premise-installed devices), the backup frequency, retention period, storage location(s), and restore method. |
| 5.3.35.2.2 | Upon contract award, the maintenance plan shall include the backup schedule and shall identify which backups are performed by the Respondent versus the Customer, including any tools, licenses, or dependencies required. |
| 5.3.35.2.3 | Upon contract award, the maintenance plan shall include the documented restoration procedures, including estimated RTOs and recovery point objectives (RPOs), for components within the Respondent's scope. Failure to meet defined RTO or RPO targets shall be subject to service level remedies in accordance with Appendix A. |

| | |
|---|---|
| 5.3.35.3 | The Respondent shall test backup restoration procedures on a scheduled basis and provide results to Customer upon request. |
| 5.3.35.3.1 | Initial backup and restoration testing shall be completed and successfully validated prior to system acceptance and cutover. |
| 5.3.35.4 | Backup jobs shall be monitored, and failures shall generate alerts and be remediated within Customer-defined timeframes. |
| 5.3.35.5 | Backup data shall be protected using encryption at rest and in transit and access shall be controlled using role-based access controls. The Customer shall retain ownership of all backup and restored data. |
| 5.3.35.6 | For hosted solutions, backup copies shall be stored in at least two (2) geographically diverse locations to support DR. |

| **5.3.36** | **Maintenance and Repair History Log** |
|---|---|
| 5.3.36.1 | The Respondent shall provide, utilize, and maintain an online history log for all Customer sites that tracks all system issues, resolutions, configuration changes, and upgrades performed onsite or remotely. The history log shall be maintained within the Respondent's ITSM or equivalent system of record. |
| 5.3.36.1.1 | The history log shall record, at a minimum, date/time, affected site(s), affected components, activity description, reason for change, personnel performing the work, and resolution status. |
| 5.3.36.1.2 | Log entries shall be created or updated in near-real time and no later than a Customer-defined timeframe (not to exceed 24 hours) after the activity occurs. |
| 5.3.36.1.3 | History log records shall be retained for a Customer-defined retention period and be searchable and exportable in Customer-approved, non-proprietary formats. |
| 5.3.36.1.4 | Customer access to the history log shall be continuously available and not limited to business hours. |
| 5.3.36.2 | The history log shall support audit and compliance reviews, including traceability to incidents, change requests, and maintenance activities. |
| 5.3.36.3 | History log entries shall reference associated trouble tickets, incidents, change requests, or escalation records where applicable. |
| 5.3.36.4 | History log data shall be protected from unauthorized modification and comply with Customer security and data-governance requirements. |
| 5.3.36.4.1 | History log records shall be immutable once finalized, with any corrections or amendments clearly identified, timestamped, and auditable. |

| **5.3.37** | **Spares and Advance Replacement** |
|---|---|
| 5.3.37.1 | The Respondent shall include a critical spares kit for all Customer-premise-installed equipment. Any spares used out from the kit shall be replaced within twenty-four (24) hours, with shipment tracking information provided to the Customer upon dispatch. |
| 5.3.37.1.1 | The contents of the critical spares kit shall be documented, itemized, and approved by the Customer prior to cutover. |
| 5.3.37.1.2 | The spares kit shall be reviewed and updated as system components change over the contract term. |
| 5.3.37.1.3 | Replacement of used spares shall not reduce spares coverage below Customer-approved minimum levels. |
| 5.3.37.2 | Upon contract award, the maintenance plan shall include a process for maintaining a readily available cache of replacement parts to be available for delivery onsite within the response timeframes outlined in Appendix A.1, Performance Standards and Terms. |
| 5.3.37.2.1 | Replacement parts caches shall be maintained in locations that support delivery within the response timeframes defined in Appendix A.1. |

| | |
|---|---|
| 5.3.37.2.2 | The Respondent shall be responsible for ensuring replacement part availability throughout the contract term, including contract extensions. |
| 5.3.37.2.3 | The Customer may request verification of replacement part availability at any time. |
| 5.3.37.3 | The Respondent shall provide pricing and documentation describing the repair and advance-replacement processes for out-of-warranty solution components purchased (versus leased) by the Customer. |
| 5.3.37.3.1 | Repair and advance-replacement timelines for out-of-warranty components shall be defined and documented. |
| 5.3.37.3.2 | Out-of-warranty component failures impacting service shall be handled with the same priority as in-warranty failures unless otherwise approved by the Customer. |
| 5.3.37.3.3 | Pricing for out-of-warranty repairs or replacements shall remain fixed for a defined period or be subject to Customer approval. |
| 5.3.37.4 | Spares and replacement parts shall align with the equipment inventory provided under Section 5.3.24, Storage, Staging, Delivery, and Inventory Control, and be updated as inventory changes. |
| 5.3.37.5 | Shipment status, tracking, and estimated delivery times for replacement parts shall be communicated proactively to the Customer. |
| 5.3.37.6 | Failure to meet replacement part delivery timelines shall trigger escalation in accordance with Section 5.3.34, Escalation Procedures. |

| **5.3.38** | **FE Documentation** |
|---|---|
| 5.3.38.1 | The Respondent shall provide documentation for all user-accessible configurations. |
| 5.3.38.1.1 | Documentation shall identify configuration dependencies, constraints, and impacts to operations or other system components. |
| 5.3.38.1.2 | Documentation shall be written in a manner suitable for operational and technical staff. |
| 5.3.38.2 | The Respondent shall provide updated documentation for all updated FE components when system updates or upgrades are applied. |
| 5.3.38.2.1 | Updated documentation shall be provided prior to or concurrent with the deployment of system updates or upgrades. |
| 5.3.38.2.2 | Documentation versioning shall clearly indicate revision history and effective dates. |
| 5.3.38.3 | The Respondent shall provide FE technician certification training and advanced technical training for interested Customer staff where applicable. |
| 5.3.38.4 | The Respondent shall provide documentation describing how the FE solution generates, exposes, and interfaces with MIS data, where applicable. |
| 5.3.38.4.1 | Documentation shall identify FE-generated data elements, interfaces, export mechanisms, and dependencies relevant to MIS or data analytics systems. |
| 5.3.38.4.2 | Detailed MIS functionality, reporting, and analytics requirements are defined in the Data Analytics requirements section of this RFP.. |
| 5.3.38.5 | The Respondent shall provide administrator guide(s) including screen layout customization; speed-dial directory maintenance, import, and export; and user account management. |
| 5.3.38.5.1 | Administrator guides shall include role-based permissions and security considerations. |
| 5.3.38.5.2 | Administrator documentation shall include backup and restore considerations for configuration data. |
| 5.3.38.6 | The Respondent shall provide telecommunicator quick reference cards for FE solutions including call handling, mapping, discrepancy reporting, and other provided systems. |

| | |
|---|---|
| 5.3.38.6.1 | Quick reference materials shall reflect Customer-specific workflows and configurations. |
| 5.3.38.6.2 | Quick reference materials shall be available in both digital and printable formats. |
| 5.3.38.7 | All documentation shall be provided in searchable electronic formats and remain accessible to the Customer for the duration of the contract. |
| 5.3.38.8 | The Respondent shall notify the Customer when documentation is updated or revised. |

| **5.3.39** | **Artificial Intelligence (AI) and Machine Learning (ML)** |
|---|---|
| 5.3.39.1 | The solution shall support AI and ML capabilities that are operationally deployed within the proposed production system and applicable to 9-1-1 and non-9-1-1 call-handling workflows. |
| 5.3.39.1.1 | AI/ML capabilities shall be clearly identified as currently available at go-live or as optional/future capabilities. |
| 5.3.39.1.2 | AI/ML functions shall not interfere with or delay live 9-1-1 call handling. |
| 5.3.39.1.3 | AI/ML outputs shall be advisory only unless explicitly approved by the Customer. |
| 5.3.39.2 | The solution shall support the use of AI/ML to assist with the handling of administrative (non-9-1-1) calls, including automated call routing, virtual attendants, call classification, or call deflection to appropriate non-emergency resources. |
| 5.3.39.2.1 | AI/ML-assisted handling of administrative calls shall include a clearly defined escalation path to a human telecommunicator. |
| 5.3.39.2.2 | AI/ML processing shall not automatically answer, delay, or block 9-1-1 calls. |
| 5.3.39.3 | The solution shall support AI/ML-based analysis of multimedia content (including text, images, audio, and video) delivered to the PSAP for purposes such as content classification, prioritization, keyword detection, or decision support. |
| 5.3.39.3.1 | AI/ML analysis of multimedia content shall preserve original media without alteration. |
| 5.3.39.3.2 | Any AI/ML-generated annotations, tags, or alerts shall be clearly identified as system-generated. |
| 5.3.39.4 | The solution shall support identification, flagging, and/or management of excessive or abusive callers, including repeat calls originating from the same location, number, or device, using AI/ML techniques and/or configurable rule-based analytics. |
| 5.3.39.4.1 | AI/ML-assisted identification of excessive or repeat calls shall not automatically block or suppress calls without human review. |
| 5.3.39.4.2 | AI/ML indicators related to repeat calls shall be advisory and visible to authorized personnel. |
| 5.3.39.5 | The Respondent shall identify how AI/ML outputs are generated and provide sufficient transparency to allow users to understand the basis of recommendations. |
| 5.3.39.6 | AI/ML processing shall comply with all applicable security, CJIS, and data-governance requirements, and shall not transmit PSAP data to unauthorized third parties. |
| 5.3.39.7 | The Customer shall have the ability to enable, disable, or limit AI/ML features by function, PSAP, or role. |
| 5.3.39.8 | Changes to AI/ML models or behavior shall follow the change management process defined in Section 5.3.21, Change Management. |

| **5.3.40** | **FE Performance Standards and SLRs** |
|---|---|
| 5.3.40.1 | The Respondent shall meet the requirements and definitions in Appendix A.1, Performance Standards and Terms. |

| | |
|---|---|
| 5.3.40.1.1 | The Respondent shall demonstrate compliance with Appendix A.1 requirements through measurable, testable performance metrics. |
| 5.3.40.1.2 | Performance standards defined in Appendix A.1 shall be enforceable contractual obligations, not aspirational targets. |
| 5.3.40.1.3 | Performance compliance shall be validated during acceptance testing and ongoing operations. |
| 5.3.40.2 | The Respondent shall meet the requirements in Appendix A.2, IP Network Measurement and Reporting Requirements. |
| 5.3.40.2.1 | IP network measurements defined in Appendix A.2 shall be collected continuously and reported in real or near-real time, where technically feasible. |
| 5.3.40.2.2 | Network performance metrics shall include, at a minimum, latency, jitter, packet loss, availability, and MOS. |
| 5.3.40.2.3 | Measurement data shall be retained for a Customer-defined period and be available for audit or regulatory reporting. |
| 5.3.40.3 | The Respondent shall meet the requirements in Appendix A.3, Service Level Agreement. |
| 5.3.40.3.1 | SLA requirements in Appendix A.3 shall apply to all components of the CHE solution, including hosted, customer-premise, and third-party integrated elements within the Respondent's control. |
| 5.3.40.3.2 | SLA compliance shall be continuously monitored and reported to the Customer. |
| 5.3.40.3.3 | Failure to meet SLA requirements shall trigger remedies as defined in Appendix A.3 without requiring a Customer request. |
| 5.3.40.4 | The Respondent shall clearly document how each SLA metric is calculated, measured, and validated. |
| 5.3.40.5 | The Customer shall have access to dashboards or reports showing current and historical performance against SLA metrics. |
| 5.3.40.6 | The Respondent shall provide a documented process for resolving disputes related to SLA measurement or compliance. |
| 5.3.40.7 | Planned maintenance windows and emergency changes shall be explicitly identified with respect to SLA applicability and exclusions. |

| **5.3.41** | **Performance, Availability, and Resiliency** |
|---|---|
| 5.3.41.1 | The system shall maintain an offline cache(i.e.: basemaps). |
| 5.3.41.2 | The system shall allow configuration of how long inactive calls remain visible. |
| 5.3.41.3 | The system shall refresh contents in application within two (2) seconds under normal conditions. |
| 5.3.41.4 | The system shall maintain responsiveness within five (5) seconds under peak load. |
| 5.3.41.5 | The system shall refresh active location updates within one (1) second. |
| 5.3.41.6 | Blank |
| 5.3.41.7 | The system shall achieve 99.999% service availability. |
| 5.3.41.8 | The system shall have no single point of failure. |
| 5.3.41.9 | The system shall support automatic failover of mapping services. |
| 5.3.41.10 | The system shall support geographically redundant deployment. |
| 5.3.41.11 | The system shall support standalone acceptance testing. |
| 5.3.41.12 | Acceptance testing shall validate performance, accuracy, and integration. |
| 5.3.41.12.1 | The FE Acceptance Test Plan shall be delivered to the Customer no less than thirty (30) calendar days prior to execution, and the Customer shall be permitted to modify, add, or remove test cases. |
| 5.3.41.12.2 | FE acceptance testing shall include validation under normal and peak operational conditions, including multiple concurrent calls, high feature density, and regional or multi-PSAP views. |

| | |
|---|---|
| 5.3.41.12.3 | If a Priority 1 or Priority 2 defect is identified during acceptance testing, the affected test cases shall be re-executed following correction. |
| 5.3.41.13 | The system shall not be accepted with unresolved Priority 1 or Priority 2 defects. |
| 5.3.41.14 | The system shall operate during third-party data feed outages. |
| 5.3.41.15 | The system shall visually indicate degraded third-party feeds. |
| 5.3.41.16 | Third-party feed failure shall not impact authoritative NG9-1-1 location. |
| 5.3.41.17 | The system shall support a degraded operational mode maintaining core functionality when non-critical services are unavailable. |

| **5.3.42** | **Security, CJIS, Audit, and Governance** |
|---|---|
| 5.3.42.1 | The system shall allow users to report errors directly from the interface and support workflow tracking for resolution. |
| 5.3.42.2 | The system shall record user interactions in an auditable log. |
| 5.3.42.3 | The system shall support role-based access controls for features and data. |
| 5.3.42.4 | The system shall track the lifecycle of discrepancy reports. |
| 5.3.42.5 | The system shall encrypt all data at rest and in transit. |
| 5.3.42.6 | The system shall log access to restricted data. |
| 5.3.42.7 | The system shall log all administrative actions related to mapping configuration in an immutable audit log. |
| 5.3.42.8 | Administrative audit logs shall include administrator identity, timestamp, and configuration changes. |
| 5.3.42.9 | The system shall support separation of duties between system administrative roles. |
| 5.3.42.10 | All exports of mapping data, images, or snapshots shall be logged with user identity and timestamp. |

| **5.3.43** | **Analytics, AI, and Data Sharing** |
|---|---|
| 5.3.43.1 | The system shall support to integrate AI/ML for data analysis. |
| 5.3.43.2 | The system shall support AI reconciliation of multiple location sources. |
| 5.3.43.3 | The system shall support integration with third-party predictive analytics or AI-based decision support tools through documented APIs. |
| 5.3.43.4 | AI-derived outputs shall display confidence indicators. |
| 5.3.43.5 | AI recommendations shall not override authoritative data automatically. |
| 5.3.43.6 | The system shall allow administrative control of AI features. |
| 5.3.43.7 | AI-assisted mapping outputs shall be logged and auditable. |
| 5.3.43.8 | AI-assisted outputs shall include an explanation of contributing data sources and confidence factors. |

| **5.3.44** | **Training and Administration** |
|---|---|
| 5.3.44.1 | The Respondent shall provide formal training for FE system users prior to system acceptance. |
| 5.3.44.2 | The system training program shall include role-specific training for call-takers, dispatchers, supervisors, mapping administrators, GIS administrators, and system administrators. |
| 5.3.44.3 | The Respondent shall provide training using multiple delivery methods, including instructor-led, recorded, and self-paced materials. |
| 5.3.44.4 | Training shall include hands-on, scenario-based exercises representative of real PSAP operations. |
| 5.3.44.5 | The Respondent shall provide a train-the-trainer program enabling Customer personnel to train users without vendor intervention. |

| | |
|---|---|
| 5.3.44.6 | The train-the-trainer program shall include formal certification of Customer trainers. |
| 5.3.44.7 | All training materials shall be provided to the Customer and licensed for unrestricted internal use. |
| 5.3.44.8 | The system shall support ongoing and refresher training for new hires, role changes, and major updates. |
| 5.3.44.9 | Training shall be provided for new or enhanced mapping capabilities. |
| 5.3.44.10 | The system shall support distinct administrative roles and system administration. |
| 5.3.44.11 | Administrators shall be able to configure permissions and access controls for functionality. |
| 5.3.44.12 | Administrators shall be able to manage external data feeds. |
| 5.3.44.13 | Administrators shall be able to configure third-party integrations. |
| 5.3.44.14 | Administrators shall be able to enable or restrict AI-driven capabilities. |
| 5.3.44.15 | The Respondent shall provide administrative documentation sufficient for Customer self-administration. |

| **5.3.45** | **Scope, Responsibility, and Governance** |
|---|---|
| 5.3.45.1 | The Respondent shall be responsible for end-to-end FE functionality, including integrations with Customer-provided CHE, CAD, GIS, NGCS, and external data sources. |
| 5.3.45.2 | The Respondent shall remain responsible for FE functionality, including integrations within the documented scope of this solicitation. Failures of third-party systems shall not relieve the Respondent of its integration obligations unless the Respondent demonstrates that such failures are outside the documented integration requirements and are not reasonably foreseen. |
| 5.3.45.3 | The Respondent shall disclose all external dependencies required for FE functionality, including APIs, data feeds, rate limits, refresh intervals, and known operational constraints. |

| **5.3.46** | **Data Ownership, Portability, and Exit Rights** |
|---|---|
| 5.3.46.1 | All Customer-generated data, including annotations, incident overlays, saved views, configuration settings, and derived outputs, shall remain the property of the Customer. |
| 5.3.46.2 | Upon request or contract termination, the Respondent shall provide the Customer access to export data in non-proprietary formats reasonably acceptable to the Customer, including standard formats where applicable. |
| 5.3.46.3 | Export of Customer mapping data shall not require proprietary tools, additional licensing, or professional services beyond reasonable administrative effort. |

| **5.3.47** | **Configuration Authority and Administrative Control** |
|---|---|
| 5.3.47.1 | Authorized Customer administrative personnel shall be able to configure, modify, and manage settings without vendor intervention or additional cost. |
| 5.3.47.2 | Administrative control shall include, at a minimum:<br>a. Data source prioritization<br>b. Visibility of additional data annotations<br>c. AI-assisted feature enablement or restriction<br>d. Regional and tenant-based configuration |
| 5.3.47.3 | Respondent approval shall not be required for routine operational or configuration changes performed by authorized Customer personnel. |

| 5.3.48 | Software Updates, Regression Protection, and Change Control |
|---|---|
| 5.3.48.1 | System updates, patches, or enhancements shall not reduce, remove, or degrade functionality that was previously accepted by the Customer. |
| 5.3.48.2 | The Respondent shall validate that updates do not introduce regressions impacting accepted functionality. |
| 5.3.48.3 | FE acceptance testing, or a Customer-approved subset thereof, shall be repeated following material updates affecting performance, accuracy, or integration. |

| 5.3.49 | Defect Management and Post-Acceptance Support |
|---|---|
| 5.3.49.1 | Defects identified after acceptance shall be classified using the same Priority 1 through Priority 4 severity definitions applied during acceptance testing. |
| 5.3.49.2 | Priority 1 and Priority 2 defects shall be remediated in accordance with contractual service levels and shall not be deferred to future releases without Customer approval. |
| 5.3.49.3 | Workarounds for Priority 1 or Priority 2 defects shall be documented and approved by the Customer. |

| 5.3.50 | Performance Measurement and Verification |
|---|---|
| 5.3.50.1 | All performance requirements shall be measured using Customer-approved test conditions, data sets, and operational scenarios. |
| 5.3.50.2 | Performance measurements shall be repeatable, observable, and auditable by Customer personnel. |
| 5.3.50.3 | Disputes regarding performance compliance shall be resolved using Customer-observed test results unless otherwise agreed upon in writing. |

| 5.3.51 | Multi-Tenant and Regional Impact Isolation |
|---|---|
| 5.3.51.1 | Operations for one PSAP, tenant, or agency shall not materially degrade performance or availability for other PSAPs or tenants. |
| 5.3.51.2 | Failures, excessive load, or misconfiguration affecting one tenant shall be isolated and contained to the extent technically feasible. |

| 5.3.52 | Disaster Recovery and Restoration |
|---|---|
| 5.3.52.1 | The Respondent shall ensure configurations, additional data, and operational settings are included in DR and backup processes. |
| 5.3.52.2 | DR procedures shall include restoration of Customer-defined configurations and saved operational data. |
| 5.3.52.3 | The Respondent shall periodically validate recovery procedures and provide documentation upon request. |

| 5.3.53 | Acceptance Authority and Go-Live Control |
|---|---|
| 5.3.53.1 | Final acceptance of the FE system shall be determined solely by the Customer. |
| 5.3.53.2 | The Customer reserves the right to delay go-live until all acceptance criteria are satisfied, independent of CHE or CAD readiness. |

| 5.3.54 | APIs and Interoperability |
|---|---|
| 5.3.54.1 | The solution shall provide documented APIs for external business intelligence (BI) tools such as Power BI and Tableau. |
| 5.3.54.2 | APIs shall conform to OpenAPI 3.0 or OData standards. |
| 5.3.54.3 | The solution shall support Customer-controlled anonymized public/open data exports. |

| | |
|---|---|
| 5.3.54.4 | The analytics solution shall continue to operate independently of FEs, CHE, CAD, GIS, or mapping system availability using the most recently ingested data. |
| 5.3.54.5 | The solution shall clearly indicate when analytics outputs are operating in a degraded or delayed-data state. |

| **5.3.55** | **Security and CJIS** |
|---|---|
| 5.3.55.1 | All data shall be encrypted in transit and at rest using AES-256 or stronger encryption. |
| 5.3.55.2 | The solution shall maintain CJIS and SOC 2 compliance for hosted and cloud deployments. |
| 5.3.55.3 | The solution shall maintain immutable audit logs for analytics data access and report activity. |

| **5.3.56** | **Administration and Governance** |
|---|---|
| 5.3.56.1 | The solution shall support distinct administrative roles for configuration, AI governance, and system administration. |
| 5.3.56.2 | Administrators shall be able to enable, disable, and govern AI models and analytics features. |
| 5.3.56.3 | Administrators shall control API access and external integrations. |
| 5.3.56.4 | The solution shall maintain version history for dashboards, reports, calculations, and AI models. |
| 5.3.56.5 | Authorized administrators shall be able to view prior versions and revert to previous configurations without Respondent involvement. |
| 5.3.56.6 | All changes to data logic, formulas, dashboards, and AI models shall be immutably logged and auditable. |

| **5.3.57** | **Training and Knowledge Transfer** |
|---|---|
| 5.3.57.1 | The Respondent shall provide formal training for analytics users, administrators, supervisors, and executives. |
| 5.3.57.2 | The solution shall include a train-the-trainer program allowing Customer personnel to independently train others. |
| 5.3.57.3 | Training materials shall be licensed for unrestricted internal Customer use. |

| **5.3.58** | **Acceptance Testing** |
|---|---|
| 5.3.58.1 | The Respondent shall support acceptance testing prior to system acceptance. |
| 5.3.58.2 | Acceptance testing shall validate data accuracy, dashboard refresh rates, AI outputs, and regulatory reports. |
| 5.3.58.3 | The solution shall not be accepted with unresolved Priority 1 or Priority 2 analytics defects. |
| 5.3.58.4 | The Respondent shall define RTOs and RPOs specific to the data solution. |
| 5.3.58.5 | Data disaster recovery shall not be dependent on FE recovery timelines. |

| **5.3.59** | **Data Ownership and Portability** |
|---|---|
| 5.3.59.1 | The Customer shall retain exclusive ownership of all data. |
| 5.3.59.2 | The solution shall support full export of historical data in non-proprietary formats upon request or contract termination. |

| **5.3.60** | **Accessibility and ADA Compliance** |
|---|---|
| 5.3.60.1 | Analytics interfaces shall comply with ADA and Web Content Accessibility Guidelines (WCAG) 2.1 Level AA. |
| 5.3.60.2 | Accessibility applies to all deployment models. |

| | |
|---|---|
| 5.3.60.3 | The system shall support keyboard navigation, screen readers, and visual accessibility. |
| 5.3.60.4 | Accessibility settings shall be configurable without Respondent intervention. |
| 5.3.60.5 | The Respondent shall disclose known accessibility limitations when awarded and include a remediation plan. |

| **5.3.61** | **Report Export and Printing** |
|---|---|
| 5.3.61.1 | Users shall be able to download reports on demand. |
| 5.3.61.2 | Reports shall be exported in PDF, Excel, or CSV. |
| 5.3.61.3 | Reports shall be print-ready with proper formatting. |
| 5.3.61.4 | Exports shall preserve filters, labels, and data accuracy. |
| 5.3.61.5 | Exports shall include report metadata. |
| 5.3.61.6 | Role-based controls shall govern report export and printing. |
| 5.3.61.7 | Exported reports shall comply with ADA/WCAG standards. |
| 5.3.61.8 | Reports shall be suitable for court and public records use. |
| 5.3.61.9 | Report export actions shall be logged immutably. |
| 5.3.61.10 | Report exports shall be completed without Respondent processing. |

## 5.4 Call-Handling Requirements

For clarity, each requirement identified in this section is associated with and shall be interpreted as part of Section 5.4, regardless of the individual Requirement ID numbering shown.

| **5.4.1** | **CHE Regulatory and i3 Standards Conformance** |
|---|---|
| 5.4.1.1 | The CHE solution shall be capable of receiving and processing 9-1-1 locations that meet FCC requirements and timelines regarding horizontal location accuracy and z-axis availability and accuracy. |
| 5.4.1.1.1 | The Respondent shall support measurement, reporting, and auditing of location accuracy and timeliness to demonstrate carrier compliance with FCC requirements. |
| 5.4.1.1.2 | The solution shall support future FCC-mandated enhancements to location accuracy, z-axis reporting, and delivery timelines in accordance with Section 5.3.7, Industry Standards Evolution. |

| **5.4.2** | **CHE Multi-Tenant Capability** |
|---|---|
| 5.4.2.1 | The Respondent shall deploy multiple tenants as necessary for the Customer's call handling solution to support its primary, backup, training, and potentially other PSAPs, if necessary, in the future. The Customer also requires training workstations to be capable of being used for live 9-1-1 call-taking if necessary. |

| **5.4.3** | **CHE Integrated Text to 9-1-1** |
|---|---|
| 5.4.3.1 | The CHE solution shall receive, present, answer, manage, and track text to 9-1-1 conversations in real time, including queueing, assignment, status, and disposition. This shall include any text to 9-1-1 conversations originating in a legacy or NG9-1-1 environment. |
| 5.4.3.1.1 | Text to 9-1-1 calls shall support equivalent priority handling, queue visibility, and supervisory monitoring as voice 9-1-1 calls. |
| 5.4.3.2 | Text to 9-1-1 calls shall be transferable between PSAPs and call-takers with full conversation history, timestamps, and associated metadata unless explicitly constrained by an external system. |
| 5.4.3.3 | The Respondent shall provide examples of the applicable UIs (e.g., screenshots) prior to system deployment. |
| 5.4.3.3.1 | The Respondent shall provide UI examples that represent production functionality available at the time of proposal or clearly identify roadmap items prior to system deployment. |

| | |
|---|---|
| 5.4.3.4 | The solution shall support outbound text messaging from the PSAP to the originating party and shall identify which additional multimedia features are currently supported versus planned. |
| 5.4.3.4.1 | Outbound text from 9-1-1 capabilities shall support policy controls, user permissions, programmable outbound display number, and audit logging. |
| 5.4.3.5 | The CHE solution shall accept Short Message Service (SMS) text delivery and associated location information via an ESInet connection using SIP with Message Session Relay Protocol (MSRP) without requiring a separate connection for SMS delivery. |
| 5.4.3.5.1 | Failure of SMS delivery components shall not impact voice call handling and shall generate alerts in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.3.6 | The CHE solution shall support conveyance of location information received with an SMS text to a mapping system. |
| 5.4.3.6.1 | Location updates received during an active text session shall be dynamically conveyed to the mapping system. |
| 5.4.3.7 | The CHE solution shall support predefined, PSAP-defined scripts for use during text transactions. |
| 5.4.3.7.1 | Predefined scripts shall be configurable by the Customer, version-controlled, and auditable. |
| 5.4.3.8 | The Respondent shall clearly identify whether SMS foreign language translation is available at contract award and provide a committed timeline for any roadmap items. |
| 5.4.3.8.1 | Translated text shall be clearly identified, and the solution shall provide disclaimers regarding automated translation accuracy. |
| 5.4.3.9 | The solution shall support transfers between different Text Control Center (TCC) providers in accordance with applicable standards and shall disclose any functional limitations. |
| 5.4.3.10 | The Respondent shall document current and planned support for Rich Communications Services (RCS) messaging and alignment with i3 and FCC guidance. Documentation shall be provided to the Customer upon request. |
| 5.4.3.11 | Text to 9-1-1 sessions shall meet defined performance thresholds for delivery, presentation, and updates consistent with voice call-handling requirements. |
| 5.4.3.12 | Text to 9-1-1 services shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. including failures in delivery, routing, or multimedia processing. |
| 5.4.3.13 | Text to 9-1-1 communications and stored content shall comply with Section 5.3.3, Security, requirements, including encryption, access controls, and audit logging. |
| 5.4.3.14 | Text to 9-1-1 functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| 5.4.4 | **CHE Real-Time Text (RTT)** |
|---|---|
| 5.4.4.1 | The Respondent shall support native RTT to 9-1-1 as a part of its solution. |
| 5.4.4.1.1 | Native RTT support shall comply with applicable FCC rules and relevant industry standards (e.g., Request for Comment [RFC] 4103, NENA i3 requirements). |
| 5.4.4.1.2 | RTT calls shall support equivalent priority handling, queueing, monitoring, transfer, recording, and logging as voice 9-1-1 calls. |
| 5.4.4.1.3 | RTT functionality shall interoperate with i3-conformant NGCS, ESInet, and neighboring PSAPs without proprietary extensions. |
| 5.4.4.2 | If native RTT is not available at contract award, the Respondent shall commit to delivering RTT support within a Customer-approved timeframe following contract execution, at no additional cost. |
| 5.4.4.2.1 | Until native RTT is available, the Respondent shall identify interim measures to support accessibility requirements without degrading service quality. |
| 5.4.4.3 | RTT functionality shall support accessibility requirements for deaf, hard-of-hearing, and speech-impaired users in accordance with ADA and FCC mandates. |
| 5.4.4.4 | RTT services shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming, including failures in RTT session establishment or delivery. |

| | |
|---|---|
| 5.4.4.5 | RTT communications shall comply with Section 5.3.3, Security, requirements, including encryption, access controls, and audit logging. |
| 5.4.4.6 | RTT functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |
| 5.4.4.7 | RTT sessions shall be recorded, retained, and exportable in accordance with Customer-defined retention policies and regulatory requirements. |

| **5.4.5** | **CHE Transcription and Translation** |
|---|---|
| 5.4.5.1 | The solution shall provide automated transcription of live 9-1-1 voice calls and recordings into a searchable text record. If third-party connectivity is required, such connectivity shall meet all security, redundancy, and monitoring requirements of this RFP. |
| 5.4.5.1.1 | Transcription latency and accuracy shall meet Customer-defined performance thresholds and be suitable for operational and evidentiary use. |
| 5.4.5.2 | The Respondent shall define transcription accuracy metrics, confidence scoring (if available), and expected transcription latency for live and recorded calls. |
| 5.4.5.2.1 | The solution shall identify when transcription confidence falls below acceptable thresholds and flag such transcripts accordingly. |
| 5.4.5.3 | The solution shall implement tagging/flagging of key words such as “gun,” “unconscious,” or “drowning” to enhance search capabilities for a minimum of 20 Customer-defined keywords. |
| 5.4.5.3.1 | Keyword tagging shall be configurable by the Customer, including the ability to add, remove, and modify keywords and phrases. |
| 5.4.5.3.2 | The solution shall support tuning or suppression of false-positive keyword tagging. |
| 5.4.5.4 | Transcripts shall include timestamps, speaker attribution (where available), and integrity controls sufficient to support admissibility in accordance with applicable state and federal evidentiary standards. |
| 5.4.5.4.1 | The Respondent shall identify any limitations or disclaimers related to transcript evidentiary use. |
| 5.4.5.5 | The Respondent shall implement logging and secure storage of transcripts to ensure accessibility and security for the Customer. |
| 5.4.5.5.1 | Transcript storage shall comply with Customer-defined retention policies, CJIS requirements, and role-based access controls. |
| 5.4.5.5.2 | Transcripts and associated metadata shall be exportable in non-proprietary formats acceptable to the Customer. |
| 5.4.5.6 | The solution shall provide real-time foreign language translation capabilities in support of audio 9-1-1 calls as well as texts to 9-1-1 and texts from 9-1-1, particularly for Spanish, Korean, Turkish, Russian, Vietnamese, Hmong, Chinese, German, Arabic, Burmese, Romanian, and Portuguese. |
| 5.4.5.6.1 | The solution shall support real-time translation for the listed languages for both audio and text interactions, and shall clearly identify which languages are available at contract award. |
| 5.4.5.6.2 | The Respondent shall identify translation accuracy expectations and limitations, including the use of automated versus human-assisted translation where applicable. |
| 5.4.5.6.3 | Failure or degradation of translation services shall not impact core call-handling functionality and shall generate alerts in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.5.7 | All translation shall be bi-directional; translations of incoming audio and text must be into English for the Customer’s telecommunicators, and responses must be translated back into the original foreign language. |
| 5.4.5.7.1 | Bi-directional translations shall preserve conversational context, sequencing, and timestamps to the extent technically feasible. |
| 5.4.5.8 | All translated conversations shall be logged and made available to authorized Customer personnel in real or near-real time. |
| 5.4.5.8.1 | Translation logs shall be searchable and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |

| | |
|---|---|
| 5.4.5.9 | The solution shall ensure that connectivity to the translation service is diverse, secure, and actively monitored for security threats. |
| 5.4.5.9.1 | Third-party translation services shall comply with Customer security requirements, including encryption, access controls, and third-party risk management practices defined in Section 5.3.3, Security. |
| 5.4.5.10 | The solution shall support the creation of pre-translated canned announcements or text messages for use by the Customer in service request contexts. |
| 5.4.5.10.1 | Pre-translated canned announcements shall be configurable by the Customer, version-controlled, and auditable. |
| 5.4.5.11 | Transcription and translation features shall support accessibility requirements in accordance with ADA and FCC mandates. |
| 5.4.5.12 | Transcription and translation services shall be monitored and alerted in accordance with these specifications and/or the SOW. |
| 5.4.5.13 | Transcription and translation functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |
| 5.4.5.14 | The Customer shall retain ownership of all transcription and translation data. Such data shall not be used to train third-party models or inform Large Language Models (LLM) without the Customer's explicit written approval. |

| **5.4.6** | **CHE Status Lights** |
|---|---|
| 5.4.6.1 | The solution shall provide real-time visual indication of call-taker status, including but not limited to busy on 9-1-1 calls, busy on administrative calls, available, and needs assistance, through on-screen indicators and/or physical status light devices. |
| 5.4.6.1.1 | Call-taker status indicators shall update in real or near-real time to reflect the current operational state. |
| 5.4.6.1.2 | Status states, colors, and labels shall be configurable by the Customer on a per-PSAP and per-tenant basis. |
| 5.4.6.1.3 | Supervisors shall have a consolidated view of call-taker status across all workstations within a PSAP. |
| 5.4.6.1.4 | Call-taker status shall automatically reflect call state changes (e.g., call answered, call released), with the ability for authorized users to manually override status when needed. |
| 5.4.6.1.5 | Status indication mechanisms shall support accessibility requirements, including configurable color schemes and alternative visual or non-visual indicators in accordance with ADA requirements. |
| 5.4.6.1.6 | Changes in call-taker status shall be logged and made available for reporting and audit purposes in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.6.2 | If physical status light devices are supported, the Respondent shall identify hardware requirements, installation considerations, and redundancy options. |
| 5.4.6.3 | Status indicators shall clearly identify the tenant and PSAP context in multi-tenant environments. |
| 5.4.6.4 | Status indication capabilities shall continue to function during partial system degradation or network failover events to the extent technically feasible. |

| **5.4.7** | **CHE User Profiles** |
|---|---|
| 5.4.7.1 | User profiles shall retain all user-specific settings, including roles, permissions, screen layouts, preferences, and accessibility settings across logins, sessions, system restarts, and upgrades. |
| 5.4.7.1.1 | User profiles shall be backed up and recoverable in accordance with system backup and recovery requirements. |
| 5.4.7.2 | The solution shall support the capability to change profile roles without having to sign out (i.e., training officer to call-taker). |
| 5.4.7.2.1 | Role changes performed without signing out shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |

| | |
|---|---|
| 5.4.7.2.2 | The ability to change roles without signing out shall be restricted to authorized users and governed by role-based access controls. |
| 5.4.7.3 | The solution shall support skills-based user profiles that enable automatic call distribution (ACD) based on call type, origin, language, and other Customer-defined criteria. |
| 5.4.7.3.1 | Skills-based routing rules shall be configurable by the Customer on a per-PSAP and per-tenant basis. |
| 5.4.7.3.2 | Supervisors shall be able to manually override skills-based routing when operationally necessary. |
| 5.4.7.4 | Profiles shall be stored on the network and be available from any workstation on the same call-handling system. |
| 5.4.7.4.1 | In the event of temporary network disruption, the solution shall support continued access to the last-known user profile configuration to the extent technically feasible. |
| 5.4.7.5 | 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, or PRF routed calls], speed dials, configurations, screen layouts, greetings, etc.) shall be controlled by a user's profile. |
| 5.4.7.5.1 | Changes to profile-based access controls shall require appropriate authorization and shall be logged and auditable. |
| 5.4.7.5.2 | Profile-based access controls shall enforce tenant and PSAP isolation in accordance with Section 5.3.11, Multi-Tenant Capability. |
| 5.4.7.6 | The solution shall provide at least one read-only user profile that permits view-only access to configurations and settings. |
| 5.4.7.7 | User profiles shall support individual accessibility settings (e.g., font size, contrast, audio cues) in accordance with ADA requirements and shall persist across sessions and upgrades. |
| 5.4.7.8 | The solution shall support provisioning, modification, suspension, and deactivation of user profiles, including automatic deactivation for inactive accounts as defined by Customer policy. |
| 5.4.7.9 | The Respondent shall provide reporting on user profiles, roles, permissions, and access changes. |

| **5.4.8** | **CHE System Availability** |
|---|---|
| 5.4.8.1 | During failover events, call-handling capacity, routing, audio quality, location delivery, and mapping functionality shall remain within defined performance thresholds. |
| 5.4.8.2 | The Respondent shall provide hot-seating capabilities, defined as the ability for a telecommunicator from one PSAP or agency to log in at a workstation at a different PSAP or agency, or from a laptop associated with a mobile PSAP, and process calls. Such capability shall be permitted only where both PSAPs/agencies are co-tenants on the same system. Upon login, the telecommunicator's "home" assets (e.g., trunks, lines, queues, speed dial lists, screen layouts, map, greetings, and related configurations) shall be fully available at the remote location. |
| 5.4.8.3 | Hot-seating shall enforce tenant, PSAP, and role-based access controls in accordance with Sections 5.3.11, Multi-Tenant Capability, and 5.4.7, CHE User Profiles. |
| 5.4.8.4 | Hot-seating logins and asset access shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |

| **5.4.9** | **CHE Recording/Instant Recall Recorder (IRR) Interoperability** |
|---|---|
| 5.4.9.1 | The CHE solution shall log all media associated with emergency calls. The CHE must support the logging of the media associated with all other calls received on any designated queue based on local capture policy. |
| 5.4.9.1.1 | Media logging shall be continuous and shall not be interrupted during failover, recovery, or degraded operating conditions. |
| 5.4.9.1.2 | Capture policies shall be configurable by the Customer and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.9.2 | The CHE solution shall support storage of audio, video, and images. |
| 5.4.9.2.1 | Recorded media shall be retained, protected, and disposed of in accordance with Customer-defined retention policies, CJIS requirements, and legal hold obligations. |

| | |
|---|---|
| 5.4.9.2.2 | Recorded media shall be exportable in non-proprietary formats acceptable to the Customer. |
| 5.4.9.3 | The Respondent shall provide the ability for remote recording and storage of PSAP audio, video or images. |
| 5.4.9.3.1 | The solution shall support secure remote recording and storage of PSAP audio, video, and images, including during remote call-taking operations. |
| 5.4.9.3.2 | Remote recording and storage shall comply with Section 5.3.3, Security, requirements, including encryption, access controls, and audit logging. |
| 5.4.9.4 | The CHE solution must support the logging of all media for calls received or placed by a particular telecommunicator, including media received from the telecommunicator's microphone and media sent to the telecommunicator's earpiece, or text or video sent or received. Logs shall be remotely accessible from a supervisor's workstation. |
| 5.4.9.4.1 | Logged media shall be correlated by agent, call, incident, and timestamp to support review and evidentiary use. |
| 5.4.9.5 | The CHE solution shall support a Session Recording Protocol interface to a logging service to record media and, if provided, metadata. This interface shall follow SIP recording (SIPREC) requirements and procedures described in RFC 6341, RFC 7865, RFC 7866, and RFC 9806. |
| 5.4.9.5.1 | SIPREC interoperability shall be validated during acceptance testing in accordance with Section 5.3.10, Solution Validation. |
| 5.4.9.5.2 | SIPREC implementations shall not require proprietary extensions for core recording functionality. |
| 5.4.9.6 | The CHE solution shall support the ability to record a separate audio channel for each participant in a call. |
| 5.4.9.6.1 | Users shall be able to selectively play, mute, or isolate individual audio channels during playback. |
| 5.4.9.7 | The CHE solution shall support an IRR that allows for the quick review of current or recent emergency communications content consisting of all media types. |
| 5.4.9.7.1 | 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. |
| 5.4.9.7.2 | IRR capability provided by the CHE solution shall allow the user to navigate within and between recalled communications. |
| 5.4.9.7.3 | Instant recall access to current or recent communications shall be available within Customer-defined time thresholds. |
| 5.4.9.7.4 | IRR access and scope shall be governed by role-based access controls and local policy. |
| 5.4.9.8 | The IRR capability provided by the CHE solution shall support transcription of emergency communications. |
| 5.4.9.8.1 | IRR transcription shall align with transcription requirements defined in Section 5.3.11, Multi-Tenant Capability, including accuracy disclosure and confidence indicators where available. |
| 5.4.9.9 | The solution shall support recording at workstations for both radio and telephony. |
| 5.4.9.9.1 | Recorded radio and telephony media shall be time-synchronized to support accurate playback and analysis. |
| 5.4.9.10 | The solution shall support playback of radio and 9-1-1 calls independently or together. |
| 5.4.9.10.1 | Users shall be able to synchronize playback of radio and 9-1-1 calls for comparative review. |
| 5.4.9.11 | 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):<br>a. Play<br>b. Pause<br>c. Stop<br>d. Play forward/fast forward (without altering voice pitch)<br>e. Rewind<br>f. Repeat<br>g. Skip forward or back a configurable number of seconds |
| 5.4.9.11.1 | Playback controls shall be configurable and support accessibility requirements in accordance with ADA. |

| | |
|---|---|
| 5.4.9.12 | The solution shall log the playback of audio recordings. |
| 5.4.9.12.1 | Playback logs shall be retained and made available for audit and review in accordance with Customer-defined retention policies. |
| 5.4.9.13 | The solution shall maintain chain-of-custody controls for recorded media, including integrity checks and access logging. |
| 5.4.9.14 | The solution shall support legal hold functionality to prevent alteration or deletion of recordings subject to litigation or investigation. |
| 5.4.9.15 | Recording and IRR services shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming, including failures or degradation of recording functionality. |
| 5.4.9.16 | Recording and IRR functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |
| | |
| **5.4.10** | **CHE PSAP Hardware** |
| 5.4.10.1 | PSAP hardware provided by the Respondent (e.g., monitors, keyboards, mice, headsets, phones) shall be new and covered by a manufacturer warranty for no less than five (5) years from the date the device is placed into operation. |
| 5.4.10.1.1 | "New" hardware shall mean unused, current-generation equipment that has not been previously deployed, refurbished, or reconditioned. |
| 5.4.10.1.2 | Manufacturer warranties shall cover parts, labor, firmware updates, and replacement or repair without service interruption. |
| 5.4.10.2 | 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. |
| 5.4.10.2.1 | Any device that does not support redundant power supplies or network interfaces shall be explicitly identified with a mitigation strategy approved by the Customer. |
| 5.4.10.3 | Universal serial bus (USB) connections on workstations shall support standard peripherals, including headsets, speakers, keypads, and accessibility devices required to meet ADA requirements. |
| 5.4.10.4 | The Respondent shall work with the Customer to provide and maintain mobile laptop call-taking positions and spares at each PSAP to be used for remote call processing. The mobile laptops shall be interchangeable between PSAPs. Spare equipment shall be ready for immediate deployment during service-impacting events. |
| 5.4.10.4.1 | The Respondent shall include a minimum 10% quantity of mobile laptops and spares provided per PSAP and ensure they are maintained in a ready-to-deploy state. |
| 5.4.10.4.2 | Mobile laptop hardware shall be included in lifecycle management, warranty, and replacement planning in accordance with Section 5.3.13, Long-Term Availability. |
| 5.4.10.5 | 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.<br>a. The headset interface shall include a volume control.<br>b. The interface shall provide audio outputs to interface to the PSAP audio enclosure used to combine radio and telephone audio into one headset.<br>Note: All wireless headsets must support encryption. |
| 5.4.10.5.1 | The Respondent shall identify supported headset models and compatibility with common PSAP audio enclosures. |
| 5.4.10.5.2 | Wireless headset encryption shall use industry-accepted standards and pairing and key management shall be secured and auditable. |
| 5.4.10.6 | The Respondent's proposed CHE solution shall interoperate with an external keypad used for dialing telephone numbers, answer/release, volume control and other telephone functions. |
| 5.4.10.6.1 | Failure of an external keypad shall not prevent call handling and shall have a defined fallback mechanism. |

| | |
|---|---|
| 5.4.10.7 | The Respondent shall standardize PSAP hardware models, where feasible, to simplify maintenance, spares, and training. |
| 5.4.10.8 | The Respondent shall document power, cooling, space, and environmental requirements for all PSAP hardware. |
| 5.4.10.9 | The Respondent shall maintain an inventory of PSAP hardware assets, including serial numbers, warranty status, and location. |
| 5.4.10.10 | PSAP hardware shall be included in acceptance and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.11** | **CHE Human Machine Interface (HMI)** |
|---|---|
| 5.4.11.1 | 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 shall take the form of a visual indication to the call-taker as described in Section 5.3.3.CC of NENA 54-750 (or its successor document when ratified). |
| 5.4.11.1.1 | Diversion indicators and associated reasons shall be logged and retained with the call record for audit and review purposes. |
| 5.4.11.1.2 | Supervisors shall have visibility into call diversion indicators across active and historical calls. |
| 5.4.11.1.3 | If SIP History-Info or Reason parameters are unavailable, the solution shall clearly indicate that diversion information is incomplete or unavailable. |

| **5.4.12** | **CHE Distinctive Ring Tones** |
|---|---|
| 5.4.12.1 | The solution shall provide the ability to configure distinctive ring tones for 9-1-1 calls, 9-1-1 calls in a pending queue, administrative calls, and text messages. |
| 5.4.12.1.1 | The solution shall support priority rules to ensure emergency 9-1-1 ring tones supersede administrative or non-emergency ring tones when simultaneous calls are present. |
| 5.4.12.1.2 | Changes to ring tone configurations shall take effect without requiring user logout or workstation restart. |
| 5.4.12.2 | The solution shall provide the ability to configure any call type (e.g., 9-1-1, 9-1-1 pending, PRF re-routed calls, administrative, text) with distinctive ring tones both audibly and via in-ear headsets. |
| 5.4.12.2.1 | Distinctive ring tones shall be consistent across workstation speakers and supported headsets unless explicitly configured otherwise by the Customer. |
| 5.4.12.2.2 | Ring tone volume levels shall be configurable and subject to minimum and maximum thresholds defined by the Customer. |
| 5.4.12.3 | The solution shall support user-selected, distinctive ring tones for each ACD queue or call type. |
| 5.4.12.3.1 | Customer administrators shall be able to restrict or define allowable ring tones for specific ACD queues or call types. |
| 5.4.12.3.2 | The solution shall support default and fallback ring tones if a user-selected ring tone is unavailable or invalid. |
| 5.4.12.4 | The solution shall provide distinctive ring tones to be customized by agent role or login. |
| 5.4.12.4.1 | Changes to role-based or login-based ring tone configurations shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.12.4.2 | Ring tone customization by role or login shall be isolated by tenant and PSAP in accordance with Section 5.3.11, Multi-Tenant Capability. |
| 5.4.12.5 | The solution shall support the ability to download ring tones and to use existing ring tones. |
| 5.4.12.5.1 | Supported ring tone file formats, size limits, and duration limits shall be defined and enforced by the solution. |
| 5.4.12.5.2 | Downloaded ring tone files shall be validated and scanned to prevent the introduction of malicious content. |
| 5.4.12.6 | Distinctive ring tones shall support accessibility requirements, including frequency ranges, volume control, and alternative notification mechanisms in accordance with ADA. |

| | |
|---|---|
| 5.4.12.7 | Distinctive ring tones shall be correlated with visual indicators in the HMI to reinforce call type recognition. |
| 5.4.12.8 | Distinctive ring tone functionality shall continue to operate during partial system degradation or failover events to the extent technically feasible. |
| 5.4.12.9 | Distinctive ring tone functionality shall be included in acceptance and regression testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.13** | **CHE Call Transfer** |
|---|---|
| 5.4.13.1 | 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 5.4.7.1 of NENA-STA-010.3f-2021, *Detailed Functional and Interface Specifications for the NENA i3 Solution* (or its successor document when ratified), to support an attended transfer by:<br>a. Establishing a conference (if not already established) with a conference bridge in the serving ESInet<br>b. Referring the emergency caller to the conference<br>c. Referring the transfer-to party to the conference<br>d. Completing the transfer |
| 5.4.13.1.1 | The solution shall provide clear visual and audible indications of transfer state and completion status to the call-taker and supervisor. |
| 5.4.13.1.2 | If any attended transfer step fails (conference bridge, referral of caller, referral of transfer-to party), the solution shall preserve the original call, notify the call-taker, and retry without dropping the call. |
| 5.4.13.1.3 | Attended transfer procedures shall be completed within Customer-defined performance thresholds suitable for emergency operations. |
| 5.4.13.2 | The solution shall support initiation of a blind transfer following the signaling and procedures described in section 5.4.7.2 of NENA-STA-010.3f-2021, *Detailed Functional and Interface Specifications for the NENA i3 Solution* (or its successor document when ratified). |
| 5.4.13.2.1 | The solution shall require confirmation prompts and display the intended destination prior to executing a blind transfer. |
| 5.4.13.2.2 | All blind transfer events shall be logged, including destination, timestamps, initiating user, and transfer outcome, in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.13.3 | 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 EIDO. The EIDO shall be sent "by reference" following the procedures described in section 5.4.7.4 of NENA-STA-010.3f-2021, *Detailed Functional and Interface Specifications for the NENA i3 Solution* (or its successor document when ratified). |
| 5.4.13.3.1 | The solution shall preserve and convey full call-associated location history, Additional Data, and telecommunicator-entered incident information in the EIDO, including timestamps and source metadata. |
| 5.4.13.3.2 | If EIDO conveyance "by reference" fails, the solution shall retry and alert in accordance with Section 5.3.5, Monitoring and Alarming, and provide a Customer-approved fallback method to convey essential incident information. |
| 5.4.13.3.3 | EIDO and Additional Data conveyance during transfer shall enforce tenant/PSAP isolation and role-based access controls in accordance with Sections 5.3.11, Multi-Tenant Capability, and 5.4.7, CHE User Profiles. |
| 5.4.13.4 | The solution shall support the transfer of emergency and administrative calls between PSAPs, internal queues, and external numbers, subject to Customer policy and access controls. |
| 5.4.13.5 | The solution shall support warm transfer workflows, including consultation with the transfer-to party prior to completing transfer, without placing the caller at risk. |
| 5.4.13.6 | When transferring to non-i3 or legacy endpoints, the solution shall preserve and convey the best available location and incident context and log any limitations. |

| | |
|---|---|
| 5.4.13.7 | Transfer failures, abnormal transfer delays, and EIDO conveyance errors shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.13.8 | Attended and blind call transfer workflows, including EIDO conveyance, shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |
| | |
| **5.4.14** | **CHE Conference Controller** |
| 5.4.14.1 | The conference controller shall enable the telecommunicator to add an outside party or inside party to an in-progress "live" call while remaining on the line, with no limitation as to what type of call the telecommunicator is handling. |
| 5.4.14.1.1 | Adding or removing conference participants shall not interrupt or degrade the original call or media streams. |
| 5.4.14.1.2 | The solution shall provide clear visual indicators showing active conference participants and their connection status. |
| 5.4.14.2 | The conference controller shall automatically control the audio levels (automatic gain control [AGC]) of the calling parties so that no degradation of voice quality occurs. |
| 5.4.14.2.1 | AGC shall function consistently across all conference participants and shall not introduce clipping, echo, or distortion. |
| 5.4.14.2.2 | Authorized users shall be able to override or adjust AGC settings in accordance with Customer policy. |
| 5.4.14.3 | The original telecommunicator shall be able to mute/unmute (i.e., disable/enable the microphone of) any party on the conference. |
| 5.4.14.3.1 | Muted participants shall receive an audible or visual indication that they are muted, where technically feasible. |
| 5.4.14.3.2 | Mute and unmute actions shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.14.4 | 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). |
| 5.4.14.4.1 | The HMI shall clearly indicate when a party's audio is disabled to prevent operator error. |
| 5.4.14.4.2 | The solution shall document and preserve in the recording metadata whether a participant's audio was muted or selectively disabled. |
| 5.4.14.5 | The original telecommunicator shall be able to select and drop any party from the conference. |
| 5.4.14.5.1 | The solution shall require confirmation before removing a participant from an active conference. |
| 5.4.14.5.2 | Participant removal events shall be logged with timestamps and initiating user information. |
| 5.4.14.6 | The original telecommunicator, or any of the conference parties, shall be able to drop out of the conference without disconnecting the original caller. |
| 5.4.14.6.1 | The solution shall provide confirmation that the original caller remains connected when a party exits the conference. |
| 5.4.14.6.2 | Conference exit behavior shall comply with call transfer and handoff policies defined by the Customer. |
| 5.4.14.7 | The conferencing feature shall support, at a minimum, any combination of up to eight parties. |
| 5.4.14.7.1 | The solution shall maintain acceptable audio quality and performance when supporting the maximum number of conference participants. |
| 5.4.14.8 | Conference audio and events shall be recorded and integrated with recording/IRR functionality in accordance with Section 5.4.9, CHE Recording/Instant Recall Recorder Interoperability. |
| 5.4.14.9 | Conference controller failures, dropped participants, and abnormal audio conditions shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.14.10 | Conference control functions shall be restricted to authorized users and governed by role-based access controls. |

| | |
|---|---|
| 5.4.14.11 | Conference controller functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.15** | **CHE Call Monitoring** |
|---|---|
| 5.4.15.1 | The solution shall allow authorized PSAP personnel to listen quietly to another telecommunicator's live conversation. |
| 5.4.15.1.1 | Call monitoring shall support all applicable media types associated with the call, including voice, RTT, and text sessions, where technically feasible. |
| 5.4.15.1.2 | The solution shall clearly indicate monitoring status to the monitoring personnel, including which calls and users are being monitored. |
| 5.4.15.2 | The solution shall support the ability to answer calls in monitoring status. |
| 5.4.15.2.1 | When a call is answered while in monitoring status, the solution shall clearly indicate whether the monitoring session has ended, transitioned, or continues concurrently. |
| 5.4.15.2.2 | Transitions between monitoring and active call handling shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.15.3 | Access to the monitoring feature shall be controlled by the authorized personnel's credentials. |
| 5.4.15.3.1 | Monitoring permissions shall be governed by role-based access controls defined by Customer policy. |
| 5.4.15.3.2 | Monitoring access permissions shall be reviewed periodically to ensure compliance with the principle of least privilege. |
| 5.4.15.4 | Monitoring shall include an option for the telecommunicator being monitored to be made aware (visually or audibly) when their call is being monitored. |
| 5.4.15.4.1 | The ability to notify telecommunicators of monitoring shall be configurable by Customer policy, including when notifications are enabled or suppressed. |
| 5.4.15.4.2 | Notification methods shall be consistent and clearly distinguishable from other alerts in the HMI. |
| 5.4.15.5 | Monitoring shall not degrade the audio quality of the call. |
| 5.4.15.5.1 | Monitoring shall not cause audio quality to fall outside defined performance thresholds for delay, jitter, packet loss, or MOS. |
| 5.4.15.6 | The Respondent shall support call-monitoring functionality for RTT sessions. |
| 5.4.15.6.1 | RTT monitoring shall allow authorized personnel to view the full conversation context, including timestamps and message sequencing. |
| 5.4.15.6.2 | Access to RTT monitoring shall be logged and restricted in accordance with Section 5.3.3, Security, requirements. |
| 5.4.15.7 | The Respondent solution shall 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. |
| 5.4.15.7.1 | Temporary notifications shall be time-bound, dismissible, and configurable by Customer policy. |
| 5.4.15.7.2 | Posting and removal of temporary notifications shall be logged and auditable. |
| 5.4.15.8 | Monitoring events and state changes shall be recorded and associated with the call record in accordance with Section 5.4.14, CHE Conference Controller. |
| 5.4.15.9 | Call monitoring shall enforce tenant and PSAP isolation in accordance with Section 5.3.11, Multi-Tenant Availability. |
| 5.4.15.10 | Call monitoring capabilities shall continue to function during failover and degraded operations to the extent technically feasible. |
| 5.4.15.11 | Call monitoring functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.16** | **CHE Call Barge-In** |
|---|---|
| 5.4.16.1 | The solution shall allow authorized PSAP personnel to listen quietly to another telecommunicator's live conversation and to mute or unmute (barge-in) while monitoring the call. |
| 5.4.16.2 | Barge-in permissions shall be governed by role-based access controls defined by Customer policy. |

| | |
|---|---|
| 5.4.16.3 | The solution shall provide clear visual indicators to all authorized users when a barge-in is active. |
| 5.4.16.4 | The solution shall allow the feature to be activated by utilizing a mouse or an easily invoked keyboard command. |
| 5.4.16.5 | Keyboard shortcuts and activation controls shall be configurable by the Customer. |
| 5.4.16.6 | The solution shall include safeguards (e.g., confirmation prompts or protected key combinations) to prevent accidental barge-in activation. |
| 5.4.16.7 | The call barge-in feature shall not degrade the audio quality of the call. |
| 5.4.16.8 | Barge-in shall not cause audio quality to fall outside defined performance thresholds for delay, jitter, packet loss, or MOS. |
| 5.4.16.9 | This feature shall be configurable to provide a tone that is audible to the telecommunicator (and not the caller) to announce the barge-in. |
| 5.4.16.10 | Barge-in tone behavior (enabled/disabled, tone type, volume) shall be configurable by Customer policy. |
| 5.4.16.11 | Audible barge-in tones shall be accompanied by a visual indication in the HMI. |
| 5.4.16.12 | The solution shall allow a telecommunicator or supervisor to become part of a three-way call with the caller and original telecommunicator. |
| 5.4.16.13 | The solution shall clearly indicate when a barge-in transitions into a three-way call or conference state. |
| 5.4.16.14 | Call control privileges during a three-way call shall be governed by Customer-defined roles and policies. |
| 5.4.16.15 | The Respondent shall support a barge-in capability for RTT sessions. |
| 5.4.16.16 | RTT barge-in shall allow authorized personnel to view and participate in the full conversation context with timestamps and message sequencing. |
| 5.4.16.17 | RTT barge-in events shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.16.18 | Barge-in events, including mute/unmute actions and participant changes, shall be recorded and associated with the call record in accordance with Section 5.4.9, CHE Recording/Instant Recall Recorder (IRR) Interoperability . |
| 5.4.16.19 | Barge-in functionality shall enforce tenant and PSAP isolation in accordance with Section 5.3.11, Multi-Tenant Capability. |
| 5.4.16.20 | Barge-in failures or abnormal behavior shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.16.21 | Call barge-in functionality, including RTT scenarios, shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.17** | **CHE Callback** |
|---|---|
| 5.4.17.1 | Callback of any 9-1-1 “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. |
| 5.4.17.1.1 | If the calling party number is unavailable, blocked, or invalid, the solution shall clearly indicate this condition and support Customer-defined fallback callback procedures. |
| 5.4.17.1.2 | Callback attempts shall be correlated to the original call record, including timestamps and outcome. |
| 5.4.17.2 | The solution shall automatically recognize and correctly format +1 and other North American Numbering Plan formats when invoking callbacks. |
| 5.4.17.2.1 | The solution shall normalize caller numbers for callback using Customer-configurable dialing rules and present the normalized number for operator review. |
| 5.4.17.3 | 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. |
| 5.4.17.3.1 | The Respondent shall validate the inclusion of “PSAP-callback” in SIP signaling during acceptance testing in accordance with Section 5.3.10, Solution Validation. |

| | |
|---|---|
| 5.4.17.4 | The solution shall use the Caller ID (CID) information to allow a callback to an administrative caller. |
| 5.4.17.4.1 | Administrative callback permissions shall be governed by role-based access controls and Customer policy. |
| 5.4.17.4.2 | Administrative callbacks shall be clearly identified in the HMI and in logs as administrative callbacks. |
| 5.4.17.5 | 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. |
| 5.4.17.5.1 | Dialing prefix insertion/deletion rules shall be configurable by Customer and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.17.5.2 | The solution shall validate dialing transformations and provide a warning if a transformation would result in an invalid number format. |
| 5.4.17.6 | The callback function shall require only a single mouse click. |
| 5.4.17.6.1 | The solution shall support Customer-configurable confirmation prompts for single-click callbacks to prevent accidental dialing. |
| 5.4.17.6.2 | Single-click callback controls shall support keyboard navigation and accessibility requirements in accordance with ADA. |
| 5.4.17.7 | The solution shall log callback attempts and outcomes (answered, no answer, busy, failed), including timestamps and initiating user, in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.17.8 | Callbacks flagged as "PSAP-callback" shall be prioritized appropriately in accordance with applicable standards and Customer policy. |
| 5.4.17.9 | Callback functionality across all supported call types shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |
| 5.4.17.10 | The solution shall support controls to prevent unauthorized callback actions and shall log suspicious callback patterns for review. |

| **5.4.18** | **CHE Abandoned Calls** |
|---|---|
| 5.4.18.1 | The solution shall provide a visual and audible indication for abandoned calls. |
| 5.4.18.1.1 | Visual and audible indications for abandoned calls shall persist until acknowledged or resolved in accordance with Customer-defined policy and shall be prioritized relative to other alerts. |
| 5.4.18.1.2 | Supervisors shall have real-time visibility into abandoned call indicators across the PSAP. |
| 5.4.18.2 | 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. |
| 5.4.18.2.1 | Callback numbers shall be normalized to ensure abandoned calls from the same originating number are correctly grouped. |
| 5.4.18.2.2 | Clearing abandoned call entries following a successful callback shall not remove the underlying call records from reports or logs. |
| 5.4.18.3 | The solution shall clear the abandoned call count display upon successful callback and answer of the telephone number. |
| 5.4.18.3.1 | A "successful callback" shall be defined as a completed connection in which the called party answers the call or responds to a callback text, as defined by Customer policy. |
| 5.4.18.4 | The solution shall provide a configurable option allowing for an automatic response to an abandoned call. |
| 5.4.18.4.1 | Automatic response behavior shall be configurable by the Customer, including response timing, message content, retry logic, and termination conditions. |
| 5.4.18.4.2 | The solution shall enforce Customer-defined limits on the number and frequency of automatic callback attempts. |
| 5.4.18.5 | The solution shall provide each individual agency with the ability to configure the automatic callback option to be enabled or disabled by the agency. |

| | |
|---|---|
| 5.4.18.5.1 | The default state of the automatic callback option shall be defined by the Customer for each agency. |
| 5.4.18.6 | 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 9-1-1). |
| 5.4.18.6.1 | The solution shall define timeout, no-response, and failure handling behavior for automated abandoned call return attempts. |
| 5.4.18.6.2 | Automated abandoned call responses shall support accessibility requirements, including compatibility with TTY/RTT and text-based responses where applicable. |
| 5.4.18.7 | 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). |
| 5.4.18.7.1 | Abandoned call event notifications shall be logged, correlated to call setup signaling, and made available for audit and reporting. |
| 5.4.18.7.2 | Repeated or abnormal abandoned call events shall generate alerts in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.18.8 | Abandoned call handling shall integrate with callback functionality defined in Section 5.4.17, CHE Callback, including single-click callback and SIP "PSAP-callback" marking where applicable. |
| 5.4.18.9 | Abandoned call events and automated responses shall be recorded or logged in accordance with Section 5.4.9, CHE Recording/Instant Recall Recorder (IRR) Interoperability, and evidentiary requirements. |
| 5.4.18.10 | Abandoned call detection, notification, automated response, and reporting shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.19** | **CHE Repeat Callers** |
|---|---|
| 5.4.19.1 | 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. |
| 5.4.19.1.1 | The number of prior calls displayed in the caller history shall be configurable by the Customer. |
| 5.4.19.1.2 | Caller numbers shall be normalized to ensure accurate identification of repeat callers across different numbering formats. |
| 5.4.19.1.3 | Access to caller history and telecommunicator notes shall be governed by role-based access controls and logged in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.19.2 | The solution shall identify the repeat call condition to the telecommunicator. |
| 5.4.19.2.1 | Repeat call indicators shall be clearly visible in the HMI and distinguishable from other alerts. |
| 5.4.19.2.2 | The threshold for identifying a repeat caller (e.g., number of calls within a defined time window) shall be configurable by the Customer. |
| 5.4.19.3 | The solution shall allow agencies to specify that new calls from the same caller (within a configurable time) shall be routed to the same telecommunicator who handled previous call(s), if that telecommunicator is available. |
| 5.4.19.3.1 | If the prior telecommunicator is unavailable, the solution shall route the call according to Customer-defined fallback routing rules. |
| 5.4.19.4 | The solution shall support identification and management of abusive repeat callers, including detection of non-service initialized (NSI) phones, TDoS patterns, and anomalous location behavior. |
| 5.4.19.4.1 | The solution shall support Customer-defined mitigation actions for abusive repeat callers, such as alerts, call treatment, or routing controls, in accordance with policy and applicable law. |
| 5.4.19.4.2 | Abusive repeat-caller activity shall be logged, monitored, and reportable in accordance with Section 5.3.5, Monitoring and Alarming. |

| | |
|---|---|
| 5.4.19.5 | Repeat caller identification shall integrate with abandoned call handling (Section 5.4.18) and callback functionality (Section 5.4.17). |
| 5.4.19.6 | Repeat-caller indicators and related notes shall be associated with call recordings and logs in accordance with Section 5.4.9, CHE Recording/Instant Recall Recorder (IRR) Interoperability. |
| 5.4.19.7 | Repeat-caller history and routing shall enforce tenant and PSAP isolation in accordance with Section 5.3.11, Multi-Tenant Capability. |
| 5.4.19.8 | Repeat-caller identification, routing, and reporting shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.20** | **CHE Call Spike/Major Incident Call Volume Screening/Call Prescreening** |
|---|---|
| 5.4.20.1 | The solution shall support identification and segregation of 9-1-1 calls associated with a major incident based on geographic location and other Customer-defined criteria. |
| 5.4.20.1.1 | Geographic call segregation shall leverage available location data sources, including LIS/LDB, device-reported location, and call metadata.. |
| 5.4.20.1.2 | Incident-based call segregation rules shall be modifiable in real or near-real time during an active incident. |
| 5.4.20.2 | The solution shall support routing of incident-related calls to separate, Customer-defined queues. |
| 5.4.20.2.1 | Incident-specific queues shall support configurable priority, overflow, and fallback routing rules. |
| 5.4.20.2.2 | Supervisors shall be able to enable, disable, and modify incident-related queueing behavior during an active event. |
| 5.4.20.3 | The solution shall support configurable auto-answer and/or auto-attendant announcements for incident-related calls to provide instructions or informational notices. |
| 5.4.20.3.1 | Auto-attendant messages shall be configurable by the Customer, time-bound, and easily updated or disabled during an incident. |
| 5.4.20.3.2 | Auto-attendant functionality shall support accessibility requirements, including compatibility with TTY/RTT and text-based messaging where applicable. |
| 5.4.20.4 | The solution shall allow callers to select menu options (e.g., keypad or equivalent input) to route their call to appropriate queues or informational paths as defined by Customer policy. |
| 5.4.20.4.1 | The solution shall define timeout, invalid input, and no-response handling behavior for caller menu selection. |
| 5.4.20.5 | The Respondent shall provide configurable virtual attendant functionality capable of prescreening incoming 9-1-1 and non-emergency calls using Customer-defined prompts and routing logic. The system shall automatically route calls based on caller input or predefined criteria to a live 9-1-1 queue, non-emergency queue, administrative or report line, alternate PSAP, overflow queue, or other designated position. |
| 5.4.20.5.1 | The virtual attendant shall provide immediate live-operator bypass and automatic fail-open routing upon timeout or system fault. It shall not introduce material delay to emergency call handling and shall not degrade location delivery, emergency signaling, system availability, or NENA i3 compliance. All interactions shall be fully logged and reportable. |
| 5.4.20.5.2 | Prescreening shall not delay or block access to a live telecommunicator for emergency calls beyond Customer-defined thresholds. |
| 5.4.20.5.3 | Prescreening rules and routing outcomes shall be configurable by the Customer and comply with applicable laws, regulations, and policy. |
| 5.4.20.6 | The solution shall allow authorized personnel to quickly activate and deactivate call spike and incident screening features. |
| 5.4.20.7 | Call spike detection, queue saturation, and prescreening performance shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.20.8 | The solution shall provide reporting on incident-related call volumes, routing decisions, prescreening outcomes, and abandoned calls. |
| 5.4.20.9 | Calls handled through call spike screening and prescreening workflows shall be recorded and logged in accordance with Section 5.4.9, CHE Recording/Instant Recall Recorder (IRR) Interoperability . |

| | |
|---|---|
| 5.4.20.10 | Call spike, incident routing, and prescreening workflows shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.21** | **CHE Real Time Queries** |
|---|---|
| 5.4.21.1 | Telecommunicators shall have the ability to query the call-handling system with international (E.164) numbers, pseudo automatic number identifications (pANIs), PSAP uniform resources identifiers (URIs), and callback numbers, along with a date/time range, to retrieve information received from those numbers, for both 9-1-1 and non-9-1-1 calls. |
| 5.4.21.1.1 | Queried numbers shall be normalized to ensure consistent retrieval across E.164, pANI, and other supported numbering formats. |
| 5.4.21.1.2 | Query results shall include call metadata, timestamps, call type, routing history, notes, location information (where available), and associated recordings. |
| 5.4.21.1.3 | Query results shall be returned within Customer-defined performance thresholds suitable for operational and investigative use. |
| 5.4.21.2 | Telecommunicators shall be able to perform queries without being on an active 9-1-1 call. |
| 5.4.21.2.1 | Access to query functionality shall be governed by role-based access controls and logged in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.21.2.2 | The solution shall support concurrent real-time queries without degrading call-handling performance. |
| 5.4.21.3 | The solution shall support the ability to associate ("pin") recorded voice conversations and other related media to query results. |
| 5.4.21.3.1 | Pinning functionality shall support all recorded media types, including voice, text, RTT, and video where applicable. |
| 5.4.21.3.2 | Pinning and unpinning actions shall be logged and auditable and shall not alter the original recorded media. |
| 5.4.21.4 | The solution shall support filtering and sorting of query results by call type, PSAP/agency, date/time, and outcome. |
| 5.4.21.5 | Query results shall be exportable in Customer-approved, non-proprietary formats. |
| 5.4.21.6 | The solution shall indicate when query results are incomplete due to data retention limits or legal holds. |
| 5.4.21.7 | Real-time query access and retrieved data shall comply with Section 5.3.3, Security, requirements, including encryption, access logging, and least-privilege enforcement. |
| 5.4.21.8 | Real-time query functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.22** | **CHE Speed Dials** |
|---|---|
| 5.4.22.1 | The solution shall provide separate and multiple speed-dial lists for each group:<br>a. System wide (all tenants)<br>b. PSAP or Agency-specific<br>c. Personnel, by role, or login ID |
| 5.4.22.1.1 | System-wide, PSAP/agency, and personal speed-dial lists shall enforce tenant and PSAP isolation in accordance with Section 5.3.11, Multi-Tenant Capability. |
| 5.4.22.2 | The system administrator shall maintain the enterprise-wide speed-dial list, while individual PSAP/agency speed-dial lists can be managed by the local PSAP system administrator. PSAPs/agencies shall not be allowed to make changes to the enterprise-wide speed-dial list. |
| 5.4.22.2.1 | All additions, deletions, and modifications to system-wide and PSAP/agency speed-dial lists shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.22.3 | Telecommunicators shall have the ability to create/maintain their own personal speed-dial lists. |
| 5.4.22.3.1 | PSAPs/agencies shall have the capability to enable or disable personal speed-dial lists by policy. |
| 5.4.22.3.2 | Authorized supervisors shall have visibility into personal speed-dial lists for audit and troubleshooting purposes. |

| | |
|---|---|
| 5.4.22.4 | Speed dials shall be accessible from the primary application window or no more than one additional window away from the primary application window. |
| 5.4.22.4.1 | Speed-dial lists shall be accessible without noticeable delay and without impacting call-handling performance. |
| 5.4.22.5 | The solution shall provide a hierarchical organization of speed dials (up to at least five [5] levels deep), in which a list entry may refer to a single speed dial or another list. |
| 5.4.22.5.1 | The Respondent shall identify any limits on the total number of speed-dial entries and hierarchical lists supported. |
| 5.4.22.6 | The solution shall allow alphanumeric entries, e.g., 1-888-911-HELP. |
| 5.4.22.6.1 | Alphanumeric entries shall be normalized and displayed consistently with the underlying dialed number. |
| 5.4.22.7 | The solution shall allow entries in E.164 format. |
| 5.4.22.7.1 | The solution shall validate E.164 formatting and alert users to invalid entries. |
| 5.4.22.8 | The solution shall allow 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). |
| 5.4.22.8.1 | Stored dialing codes and PINs shall be protected in accordance with Section 5.3.3, Security, requirements. |
| 5.4.22.9 | Telecommunicators shall not need to take any action to immediately access speed-dial list changes. |
| 5.4.22.9.1 | The solution shall notify administrators if speed-dial updates fail to propagate. |
| 5.4.22.10 | The solution shall support the association of images and notes with each contact on the speed dial list. |
| 5.4.22.10.1 | The use of images and notes shall be governed by Customer policy and auditable. |
| 5.4.22.11 | 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). |
| 5.4.22.11.1 | Speed-dial displays shall support accessibility requirements, including keyboard navigation and screen-reader compatibility. |
| 5.4.22.12 | 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 pop-up window) of a user-selectable set of fields when the mouse pointer hovers over the button. |
| 5.4.22.12.1 | Fields displayed in hover pop-ups shall be configurable by the Customer. |
| 5.4.22.13 | The solution shall support entry, modification, and removal of additional metadata associated with speed-dial entries. |
| 5.4.22.14 | The solution shall support search functionality for speed-dial entries, including search-as-you-type. |
| 5.4.22.14.1 | Search shall support name, number, notes, and associated metadata fields. |
| 5.4.22.15 | The solution shall support uploading and using Customer-provided icons, graphics, and images for speed-dial buttons. |
| 5.4.22.15.1 | Supported file formats, sizes, and dimensions for icons shall be defined and enforced. |
| 5.4.22.16 | 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. |
| 5.4.22.16.1 | Location-based speed-dial population shall update automatically when caller location changes. |
| 5.4.22.17 | The solution shall support a minimum of ten (10) speed-dial entries per service area. |
| 5.4.22.18 | The solution shall support intelligent manipulation of dialed digits, including local, national, and international dialing normalization. |
| 5.4.22.18.1 | The normalized dialed number shall be displayed to the telecommunicator prior to call placement. |
| 5.4.22.19 | The solution shall support import and export of speed-dial lists using standard formats such as CSV, SQL, and XML. |
| 5.4.22.19.1 | Imported speed-dial data shall be validated prior to acceptance, with error reporting for invalid entries. |

| | |
|---|---|
| 5.4.22.20 | Calls initiated via speed dials shall be logged and identifiable in call records and reports. |
| 5.4.22.21 | Failures in speed-dial resolution or dialing shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.22.22 | Speed-dial functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.23** | **CHE ACD** |
|---|---|
| 5.4.23.1 | The solution shall permit trained and authorized Customer staff (by role) to provision ACD-related queues, routing, and telecommunicator skill settings, as needed. |
| 5.4.23.1.1 | ACD provisioning actions shall be governed by role-based access controls and logged in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.23.1.2 | The solution shall provide preview and confirmation of ACD configuration changes prior to activation. |
| 5.4.23.2 | 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): |
| 5.4.23.2.1 | Supported algorithms shall include, at a minimum: longest idle, top-down, round-robin, and ring-all. |
| 5.4.23.2.2 | The solution shall document and display the active ACD algorithm for each queue. |
| 5.4.23.2.3 | Authorized supervisors shall be able to temporarily override ACD algorithms during major incidents or staffing shortages. |
| 5.4.23.3 | The solution shall support ACD queueing based on call type, including wireline, wireless, VoIP, text, and other Customer-defined types. |
| 5.4.23.3.1 | ACD routing shall support additional criteria such as language, skills, location, and priority where applicable. |
| 5.4.23.4 | The solution shall provide the ability to change roles without having to log out and log back in. |
| 5.4.23.4.1 | Role changes performed without logout shall be logged and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.23.5 | The solution shall display to a telecommunicator the number of calls in each queue. |
| 5.4.23.5.1 | Queue displays shall include indicators of longest wait time or priority level where applicable. |
| 5.4.23.6 | 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. |
| 5.4.23.6.1 | The solution shall support automatic state transitions based on call handling activity and Customer-defined policy. |
| 5.4.23.7 | 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.” |
| 5.4.23.7.1 | Reason codes shall be configurable by the Customer and reportable in MIS outputs. |
| 5.4.23.8 | In a “longest idle” ACD environment, switching to “not ready” shall not reset the timer used to determine “longest idle” status. |
| 5.4.23.8.1 | The solution shall display idle-time status or relative position in the queue to authorized users where appropriate. |
| 5.4.23.9 | The solution shall support a configurable forced-answer option for ACD calls, allowing calls to be connected to the next available telecommunicator without manual acceptance. |
| 5.4.23.9.1 | Forced-answer behavior shall be configurable by the Customer, including per-queue enablement, audible alert timing, and opt-out scenarios. |
| 5.4.23.9.2 | Forced answer alerts shall support accessibility requirements, including visual cues in the HMI. |
| 5.4.23.10 | 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. |

| | |
|---|---|
| 5.4.23.10.1 | Wrap-up duration limits shall be configurable by the Customer, including minimums and maximums. |
| 5.4.23.10.2 | Supervisors shall be able to override or terminate wrap-up periods during high call volume events. |
| 5.4.23.11 | 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. |
| 5.4.23.11.1 | Telecommunicator-recorded greetings shall be subject to Customer-defined approval and quality standards. |
| 5.4.23.11.2 | Recorded greetings shall be retained and managed in accordance with Customer-defined retention policies. |
| 5.4.23.12 | ACD performance metrics (e.g., average answer time, queue depth, abandonment rate) shall be monitored and reported in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.4.23.13 | ACD functionality shall integrate with call spike and major incident screening features defined in Section 5.4.20, CHE Call Spike/Major Incident Call Volume Screening/Call Prescreening. |
| 5.4.23.14 | ACD queues, routing rules, and statistics shall enforce tenant and PSAP isolation in accordance with Section 5.3.11, Multi-Tenant Capability. |
| 5.4.23.15 | ACD configurations and routing behaviors shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.4.24** | **CHE Training** |
|---|---|
| 5.4.24.1 | The Respondent shall provide a training simulator for hands-on in-person training that can be customized to user setup. This would include capabilities to demonstrate all functionality within the system that is implemented at the PSAPs. |
| 5.4.24.1.1 | The training simulator shall mirror the Customer's production configuration without impacting live operations. |
| 5.4.24.1.2 | The Respondent shall provide a dedicated training simulator fully integrated with the proposed CHE that can generate and manage simulated calls without impacting live 9-1-1 operations. |
| 5.4.24.1.3 | The training simulator shall support generation of all call types supported by the production CHE, including wireline, wireless, VoIP, text to 9-1-1 (SMS and RTT), administrative, and non-emergency calls. |
| 5.4.24.1.4 | The training simulator shall support abandoned call scenarios, repeat caller scenarios, callbacks, transfers, conferences, call monitoring, and barge-in scenarios. |
| 5.4.24.1.5 | The training simulator shall support call spikes and major incident scenarios, including simultaneous delivery of multiple calls to multiple positions. |
| 5.4.24.1.6 | The training simulator shall support simulated delivery of Additional Data, including EIDOs conveyed "by value" and "by reference." |
| 5.4.24.1.7 | The training simulator shall support simulated location delivery, including rebids, updates, uncertainty, and z-axis data, where supported by the CHE. |
| 5.4.24.1.8 | The training simulator shall operate in a logically or physically isolated training environment that mirrors production configuration and prevents live call contamination. |
| 5.4.24.1.9 | The training simulator shall use the same user interfaces, workflows, queues, roles, profiles, and permissions as the live FE environment. |
| 5.4.24.1.10 | The training simulator shall allow instructors to script, trigger, pause, modify, replay, and terminate training scenarios in real time. |
| 5.4.24.1.11 | The training simulator shall clearly and unmistakably identify all simulated calls to users and within recordings. |
| 5.4.24.1.12 | The training simulator shall support recording, playback, and review of simulated calls for training and evaluation purposes. |
| 5.4.24.1.13 | The training simulator shall ensure simulated calls do not generate live operational, regulatory, MIS, CAD, or FCC records unless explicitly configured for training analytics. |

| | |
|---|---|
| 5.4.24.1.14 | The training simulator shall support configurations to match Customer-specific PSAP layouts, queues, call flows, and GIS boundaries. |
| 5.4.24.1.15 | The training simulator shall remain functionally aligned with CHE software upgrades and new features throughout the contract term. |
| 5.4.24.1.16 | The training simulator shall be available for initial training, refresher training, remedial training, and post-cutover testing. |
| 5.4.24.1.17 | The training simulator shall be included as a fully supported component of the proposed solution for the duration of the contract. |

| **5.4.25** | **CHE Project Management and Progress Reports** |
|---|---|
| 5.4.25.1 | The Respondent shall track and report progress of MSAG/ALI data migration and GIS data uploads to support i3 readiness. The Respondent shall achieve and maintain a minimum 98% match rate between GIS road centerlines and legacy MSAG/ALI data until such time as this process is replaced by the Location Validation Function (LVF). Upon transition to LVF, the Respondent shall provide equivalent discrepancy reporting and resolution tracking using LVF-generated reports. |

| **5.4.26** | **CHE Systems Integration** |
|---|---|
| 5.4.26.1 | The Respondent shall integrate local administrative lines (analog or SIP-based) into the CHE solution that includes the ability to access outside lines for local, nationwide, and international dialing. |
| 5.4.26.1.1 | Administrative lines (analog or SIP-based) shall be fully integrated into the CHE solution for inbound and outbound calling. |
| 5.4.26.1.2 | Porting of administrative lines shall be coordinated to avoid service interruption. |
| 5.4.26.1.3 | Outgoing administrative line configuration shall be configurable by the Customer. |
| 5.4.26.2 | The number for the in-use administrative line shall be clearly visible to the call-taker. |
| 5.4.26.2.1 | Administrative line number visibility shall persist across sessions and workstation logins. |

| **5.4.27** | **Call-Handling System Acceptance Testing** |
|---|---|
| 5.4.27.1 | The Customer's CHE acceptance testing is intended to validate overall system performance, especially system-level functionality not otherwise verifiable during individual PSAP acceptance testing and includes (but will not be limited to) testing of areas such as the following:<br>a. Inter-PSAP transfers and conferences<br>b. Automatic system failover and maintenance of full system functionality when a redundant element is taken out of service<br>c. Alternate routing under functional element and network component failure scenarios<br>d. High call volume performance |
| 5.4.27.2 | Call-handling system acceptance testing cannot begin until the Customer has successfully completed PSAP call-handling acceptance testing. The testing period shall be sufficient to demonstrate the solution's performance and reliability. The period shall be thirty (30) consecutive calendar days with zero Priority 1 and zero Priority 2 faults present or outstanding at any time during the testing period. |

| 5.4.28 | **Text, Video, and Multimedia Integration** |
|---|---|
| 5.4.28.1 | The system shall integrate with text to 9-1-1 mapping. |
| 5.4.28.2 | The system shall support outbound texts from 9-1-1 from the map. |
| 5.4.28.3 | The system shall support rapid device locate with mapped results. |
| 5.4.28.4 | The system shall support secure video streaming with mapped caller location. |
| 5.4.28.5 | The system shall visually indicate the availability and status of associated multimedia content on the map. |

## 5.5 Dispatch Mapping Requirements

For clarity, each requirement identified in this section is associated with and shall be interpreted as part of Section 5.5, regardless of the individual Requirement ID numbering shown.

| 5.5.1 | Mapping Deployment Architecture |
|---|---|
| 5.5.1.1 | The Call/Dispatch Mapping system shall support deployment in either a Customer-approved cloud environment or a Customer-approved on-premises environment, without reduction in functionality, performance, security, resiliency, or compliance. |
| 5.5.1.2 | All requirements in General Technical Requirements shall apply equally to cloud-hosted and on-premises deployments. The deployment model shall not be used to justify reduced capability, degraded performance, or limited feature availability. |
| 5.5.1.3 | The Respondent shall identify the proposed deployment architecture, including hosting responsibility, redundancy model, scaling approach, and disaster recovery strategy. |

| 5.5.2 | Mapping Core Map Interaction & Visualization |
|---|---|
| 5.5.2.1 | The system shall provide a control to reset the map view to the default or PSAP boundary extent with a single action. |
| 5.5.2.2 | The system shall provide a full-screen mode to maximize operational workspace during high-load events. |
| 5.5.2.3 | The system shall allow users to disable automatic map centering during incident updates or call movements. |
| 5.5.2.4 | The system shall allow users to zoom the map in or out using configurable zoom controls or mouse functions. |
| 5.5.2.5 | The system shall allow users to select between dark and light map display themes suitable for PSAP lighting conditions. |
| 5.5.2.6 | The system shall allow users to save and recall favorite map views or extents. |
| 5.5.2.7 | The system shall allow return to previous map views up to ten (10)minimum steps. |
| 5.5.2.8 | The system shall persist user-specific map preferences across sessions. |

| 5.5.3 | Mapping GIS Layers, Data, and Basemaps |
|---|---|
| 5.5.3.1 | The system shall allow users to toggle the visibility of GIS layers and support layer grouping and transparency controls. |
| 5.5.3.2 | The system shall display all GIS data associated with a selected point, including address, coordinates, and jurisdictional boundaries. |
| 5.5.3.3 | The system shall allow adjustment of layer transparency and organization by functional category. |
| 5.5.3.4 | The system shall display the date and time GIS data and live feeds were last refreshed by layer. |
| 5.5.3.5 | The system shall consume live GIS services from ArcGIS Server, ArcGIS Online, or other Open Geospatial Consortium (OGC)-compliant sources. |
| 5.5.3.6 | The system shall allow loading of locally maintained GIS datasets without re-publishing services. |
| 5.5.3.7 | The system shall support tenant-based map configurations. |
| 5.5.3.8 | The system shall provide administrative tools for GIS updates. |
| 5.5.3.9 | The system shall allow the viewing of GIS layer metadata. |
| 5.5.3.10 | The system shall include caching and optimization controls. |
| 5.5.3.11 | Administrators shall be able to designate authoritative GIS layers and visually distinguish them from reference layers. |

| 5.5.4 | Mapping Call, Incident, and Responder Visualization |
|---|---|
| 5.5.4.1 | The system shall display movement paths (breadcrumbs) for calls, responding units, or mobile assets and allow users to toggle this feature on or off. |
| 5.5.4.2 | The system shall display all active calls within and across jurisdictions to support situational awareness for all PSAP/Tenants. |

| | |
|---|---|
| 5.5.4.3 | The system shall support map-based call creation and integration with the CAD system for call record initiation. |
| 5.5.4.4 | The system shall display responder unit locations in real time using CAD or global positioning system (GPS) feeds. |
| 5.5.4.5 | The system shall display updated caller locations during CHE rebids with breadcrumb trails. |
| 5.5.4.6 | The system shall allow replay of prior incidents including unit movement. |
| 5.5.4.7 | The system shall provide a regional map view across multiple PSAPs. |
| 5.5.4.8 | The system shall allow filtering and viewing of calls by agency, type, or region. |
| 5.5.4.9 | The system shall allow acceptance or rejection of updated locations. |
| 5.5.4.10 | The system shall display timestamps for caller location updates, unit movement, and mapping events. |
| 5.5.4.11 | The system shall support at least one thousand (1,000) active map features. |
| **5.5.5** | **Mapping Measurement, Drawing, and Analysis Tools** |
| 5.5.5.1 | The system shall provide tools to draw, label, modify, and delete perimeters, staging areas, or annotation points on the map. |
| 5.5.5.2 | The system shall calculate distance between two or more points and allow polygon or area measurement. |
| 5.5.5.3 | The system shall allow users to create radius buffers or geofences around incidents. |
| 5.5.5.4 | The system shall provide polygon area measurement tools. |
| 5.5.5.5 | The system shall allow saving and reuse of map annotations. |

| | |
|---|---|
| **5.5.6** | **Mapping Routing, Assets, and External Awareness** |
| 5.5.6.1 | The system shall generate turn-by-turn directions for responders and display estimated travel routes and estimated times of arrival (ETAs). |
| 5.5.6.2 | The system shall link live camera feeds to mapped points for real-time situational awareness. |
| 5.5.6.3 | The system shall display live weather and traffic overlays. |
| 5.5.6.4 | Routes and ETAs shall dynamically update based on changing traffic, closures, or incident conditions. |

| | |
|---|---|
| **5.5.7** | **Mapping Location Sources, Validation, and Accuracy** |
| 5.5.7.1 | The system shall integrate what3words addressing to display precise three-meter square location identifiers. |
| 5.5.7.2 | The system shall display automatic crash notifications (eCall or telematics feeds) and map the incident location in real time. |
| 5.5.7.3 | The system shall accept, decode, and display device-based, network-based, and third-party location signals in real time. |
| 5.5.7.4 | The system shall allow searching by coordinates, civic address, place name, or alternative location providers. |
| 5.5.7.5 | The system shall allow users to identify which PSAP, law, fire, and EMS boundaries serve any selected map point. |
| 5.5.7.6 | The system shall validate addresses against authoritative NG9-1-1 GIS/LVF datasets, where available. |
| 5.5.7.7 | The system shall support custom locators and prioritization of location providers. |
| 5.5.7.8 | The system shall display multiple search results with confidence scores. |
| 5.5.7.9 | The system shall display visual indicators of positional accuracy. |
| 5.5.7.10 | The system shall display the origin of location data. |
| 5.5.7.11 | The system shall display synchronization status with NG9-1-1 GIS core services. |
| 5.5.7.12 | The system shall display the active priority order of location sources and indicate when fallback sources are used. |

| 5.5.8 | Mapping 3D, Indoor, and Z-Axis Operations |
|---|---|
| 5.5.8.1 | The system shall display multilevel building floor data and allow users to filter visible levels for indoor (z-axis) dispatch operations. |
| 5.5.8.2 | The system shall enable terrain or structure elevation viewing and support z-axis visualization for NG9-1-1 operations. |
| 5.5.8.3 | The system shall display z-axis location data with accuracy indicators. |
| 5.5.8.4 | The system shall convert 3D coordinates to 2D for CAD integration. |
| 5.5.8.5 | The system shall comply with NENA-REQ-003.1-2022 requirements for 3D GIS. |
| 5.5.8.6 | The system shall allow the configuration of z-axis visual representation. |

| 5.5.9 | Mapping Text, Video, and Multimedia Integration |
|---|---|
| 5.5.9.1 | The system shall integrate with text to 9-1-1 mapping. |
| 5.5.9.2 | The system shall support outbound texts from 9-1-1 from the map. |
| 5.5.9.3 | The system shall support rapid device locate with mapped results. |
| 5.5.9.4 | The system shall support secure video streaming with mapped caller location. |
| 5.5.9.5 | The system shall visually indicate the availability and status of associated multimedia content on the map. |

| 5.5.10 | Mapping Performance, Availability, and Resiliency |
|---|---|
| 5.5.10.1 | The Respondent shall provide a Mapping Acceptance Test Plan specific to the Call/Dispatch Mapping system. |
| 5.5.10.1.1 | The Mapping Acceptance Test Plan shall include test cases validating, at a minimum:<br>a. Map rendering and refresh performance<br>b. Location accuracy, confidence indicators, and source attribution<br>c. GIS layer visibility, authority designation, and synchronization<br>d. Live location updates, breadcrumb trails, and rebid handling<br>e. Integration with CHE, CAD, and external location or data feeds<br>f. Offline basemap operation and degraded-mode functionality<br>g. Role-based access controls and data visibility<br>h. Audit logging of mapping actions and administrative changes |
| 5.5.10.1.2 | Mapping acceptance testing shall be conducted using Customer-configured GIS data, boundaries, layers, workflows, and external data sources. |
| 5.5.10.1.3 | Mapping acceptance testing shall include validation under normal and peak operational conditions, including multiple concurrent calls, high feature density, and regional or multi-PSAP map views. |

| 5.5.11 | Mapping Security, CJIS, Audit, and Governance |
|---|---|
| 5.5.11.1 | The system shall support private, group, or global visibility of map annotations. |
| 5.5.11.2 | The system shall enforce role-based GIS visibility. |
| 5.5.11.3 | The system shall support masking of sensitive GIS layers. |
| 5.5.11.4 | The system shall encrypt all mapping data at rest and in transit. |
| 5.5.11.5 | The system shall log access to restricted mapping data. |
| 5.5.11.6 | The system shall log all administrative actions related to mapping configuration in an immutable audit log. |
| 5.5.11.7 | Administrative audit logs shall include administrator identity, timestamp, and configuration changes. |
| 5.5.11.8 | The system shall support separation of duties between mapping, GIS, and system administrative roles. |
| 5.5.11.9 | All exports of mapping data, images, or snapshots shall be logged with user identity and timestamp. |

| 5.5.12 | Mapping Analytics, AI, and Data Sharing |
|---|---|
| 5.5.12.1 | The system shall support the integration of AI/ML for geospatial analysis. |
| 5.5.12.2 | The system shall support AI reconciliation of multiple location sources. |

| 5.5.13 | Mapping Training and Administration |
|---|---|
| 5.5.13.1 | Administrators shall be able to manage GIS layers, basemaps, and default extents. |
| 5.5.13.2 | Administrators shall be able to define governance policies for map annotations. |
| | |

| 5.5.14 | Configuration Authority and Administrative Control |
|---|---|
| 5.5.14.1 | Administrative control shall include, at a minimum:<br>a. Authoritative GIS layer designation<br>b. Location source prioritization<br>c. Visibility of layers and annotations<br>d. AI-assisted mapping feature enablement or restriction<br>e. Regional and tenant-based configuration |

| 5.5.15 | Integrated Text-to-9-1-1 |
|---|---|
| 5.5.15.1 | The CHE solution shall receive, present, answer, manage, and track Text-to-9-1-1 conversations in real time, including queueing, assignment, status, and disposition. This shall include any Text-to-9-1-1 conversations originating in a legacy or NG9-1-1 environments. |
| 5.5.15.1.1 | Text-to-9-1-1 calls shall support equivalent priority handling, queue visibility, and supervisory monitoring as voice 9-1-1 calls. |
| 5.5.15.2 | Text-to-9-1-1 calls shall be transferable between PSAPs and call-takers with full conversation history, timestamps, and associated metadata unless explicitly constrained by an external system. |
| 5.5.15.3 | The Respondent shall provide examples of the applicable UIs (e.g., screenshots) prior to system deployment. |
| 5.5.15.3.1 | The Respondent shall provide UI examples that represent production functionality available at the time of proposal or clearly identify roadmap items prior to system deployment. |
| 5.5.15.4 | The solution shall support outbound text messaging from the PSAP to the originating party and shall identify which additional multimedia features are currently supported versus planned. |
| 5.5.15.4.1 | Outbound Text-from-9-1-1 capabilities shall support policy controls, user permissions, programmable outbound display number, and audit logging. |
| 5.5.15.5 | The CHE solution shall accept SMS text delivery and associated location information via an ESInet connection using SIP with MSRP without requiring a separate connection for SMS delivery. |
| 5.5.15.5.1 | Failure of SMS delivery components shall not impact voice call handling and shall generate alerts in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.5.15.6 | The CHE solution shall support conveyance of location information received with an SMS text to a mapping system |
| 5.5.15.6.1 | Location updates received during an active text session shall be dynamically conveyed to the mapping system. |
| 5.5.15.7 | The CHE solution shall support predefined, PSAP-defined scripts for use during text transactions. |
| 5.5.15.7.1 | Predefined scripts shall be configurable by Customer, version-controlled, and auditable. |
| 5.5.15.8 | The Respondent shall clearly identify whether SMS foreign language translation is available at contract award and provide a committed timeline for any roadmap items. |
| 5.5.15.8.1 | Translated text shall be clearly identified, and the solution shall provide disclaimers regarding automated translation accuracy. |
| 5.5.15.9 | The solution shall support transfers between different Text Control Center (TCC) providers in accordance with applicable standards and shall disclose any functional limitations. |
| 5.5.15.10 | The Respondent shall document current and planned support for Rich Communications Services (RCS) messaging and alignment with i3 and FCC guidance. Documentation shall be provided to Customer upon request. |

| | |
|---|---|
| 5.5.15.11 | Text to 9-1-1 sessions shall meet defined performance thresholds for delivery, presentation, and updates consistent with voice call-handling requirements. |
| 5.5.15.12 | Text to 9-1-1 services shall be monitored and alerted in accordance with Section 5.3.5, Monitoring and Alarming, including failures in delivery, routing, or multimedia processing. |
| 5.5.15.13 | Text to 9-1-1 communications and stored content shall comply with Section 5.3.3, Security, requirements, including encryption, access controls, and audit logging. |
| 5.5.15.14 | Text to 9-1-1 functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |

| **5.5.16** | **Transcription and Translation** |
|---|---|
| 5.5.16.1 | The solution shall provide automated transcription of live 9-1-1 voice calls and recordings into a searchable text record. If third-party connectivity is required, such connectivity shall meet all security, redundancy, and monitoring requirements of this RFP. |
| 5.5.16.1.1 | Transcription latency and accuracy shall meet Customer-defined performance thresholds and be suitable for operational and evidentiary use. |
| 5.5.16.2 | The Respondent shall define transcription accuracy metrics, confidence scoring (if available), and expected transcription latency for live and recorded calls. |
| 5.5.16.2.1 | The solution shall identify when transcription confidence falls below acceptable thresholds and flag such transcripts accordingly. |
| 5.5.16.3 | The solution shall implement tagging/flagging of key words such as “gun”, “unconscious”, “drowning” to enhance search capabilities for a minimum of 20 customer defined keywords. |
| 5.5.16.3.1 | Keyword tagging shall be configurable by Customer, including the ability to add, remove, and modify keywords and phrases. |
| 5.5.16.3.2 | The solution shall support tuning or suppression of false-positive keyword tagging. |
| 5.5.16.4 | Transcripts shall include timestamps, speaker attribution (where available), and integrity controls sufficient to support admissibility in accordance with applicable state and federal evidentiary standards. |
| 5.5.16.4.1 | The Respondent shall identify any limitations or disclaimers related to transcript evidentiary use. |
| 5.5.16.5 | The solution shall implement logging and secure storage of transcripts to ensure accessibility and security for Customer. |
| 5.5.16.5.1 | Transcript storage shall comply with Customer-defined retention policies, CJIS requirements, and role-based access controls. |
| 5.5.16.5.2 | Transcripts and associated metadata shall be exportable in non-proprietary formats acceptable to Customer. |
| 5.5.16.6 | The solution shall provide real-time foreign language translation capabilities in support of audio 9-1-1 calls as well as texts to 9-1-1 and texts from 9-1-1; particularly for the languages of Spanish, Korean, Turkish, Russian, Vietnamese, Hmong, Chinese, German, Arabic, Burmese, Romanian, and Portuguese. |
| 5.5.16.6.1 | The solution shall support real-time translation for the listed languages for both audio and text interactions, and shall clearly identify which languages are available at contract award |
| 5.5.16.6.2 | The solution shall identify translation accuracy expectations and limitations, including use of automated versus human-assisted translation where applicable. |
| 5.5.16.6.3 | Failure or degradation of translation services shall not impact core call-handling functionality and shall generate alerts in accordance with Section 5.3.5, Monitoring and Alarming. |
| 5.5.16.7 | All translation shall be bi-directional; translations of incoming audio/text must be into English for Customer’s telecommunicators, and responses must be translated back into the original foreign language. |
| 5.5.16.7.1 | Bi-directional translations shall preserve conversational context, sequencing, and timestamps to the extent technically feasible. |
| 5.5.16.8 | All translated conversations shall be logged and made available to authorized Customer personnel in real or near-real time. |
| 5.5.16.8.1 | Translation logs shall be searchable and auditable in accordance with Section 5.3.5, Monitoring and Alarming. |

| | |
|---|---|
| 5.5.16.9 | The solution shall ensure that connectivity to the translation service is diverse, secure, and actively monitored for security threats. |
| 5.5.16.9.1 | Third-party translation services shall comply with Customer security requirements, including encryption, access controls, and third-party risk management practices defined in Section 5.3.3, Security. |
| 5.5.16.10 | The solution shall support the creation of pre-translated canned announcements or text messages for use by Customer in service request contexts. |
| 5.5.16.10.1 | Pre-translated canned announcements shall be configurable by Customer, version-controlled, and auditable. |
| 5.5.16.11 | Transcription and translation features shall support accessibility requirements in accordance with ADA and FCC mandates. |
| 5.5.16.12 | Transcription and translation services shall be monitored and alerted in accordance with this RFP and/or the SOW. |
| 5.5.16.13 | Transcription and translation functionality shall be included in acceptance, regression, and validation testing in accordance with Section 5.3.10, Solution Validation. |
| 5.5.16.14 | Customer shall retain ownership of all transcription and translation data. Such data shall not be used to train third-party models or inform LLM without Customer's explicit written approval. |

## 5.6 NG9-1-1 Data Analytics, Reporting, and Intelligence Requirements

For clarity, each requirement identified in this section is associated with and shall be interpreted as part of Section 5.6, regardless of the individual Requirement ID numbering shown.

| **5.6.1** | **Analytics Deployment Architecture** |
|---|---|
| 5.6.1.1 | All Section 5.6 requirements apply equally to cloud and on-premises deployments. |
| 5.6.1.2 | The solution shall support cloud or on-premises deployment without the loss of functionality. |
| 5.6.1.3 | On-premises deployments shall support high availability and redundancy. |
| 5.6.1.4 | Cloud deployments shall support elastic scaling, redundancy, and U.S. data residency. |
| 5.6.1.5 | The Respondent shall document the deployment architecture and DR approach. |

| **5.6.2** | **Analytics Scope and Independence** |
|---|---|
| 5.6.2.1 | The MIS/data analytics solution shall operate as a standalone, vendor-agnostic analytics platform capable of being awarded, deployed, and operated independently of CHE, CAD, GIS, or mapping solutions. |
| 5.6.2.2 | The Customer shall retain full ownership of all raw, derived, aggregated, and analytic data, regardless of hosting or award structure. |

| **5.6.3** | **Analytics Data Integration and Normalization** |
|---|---|
| 5.6.3.1 | The solution shall automatically ingest and synchronize data real time or near real time from CHE, CAD, GIS, text to 9-1-1, RTT, and NGCS systems. |
| 5.6.3.2 | The solution shall implement a normalized NG9-1-1 data schema compliant with NENA-STA-010.3, *NENA i3 Standard for Next Generation 9-1-1*, and NENA-STA-021.1, *NENA Standard for Emergency Incident Data Object (EIDO)*, (or successor standards when ratified). |
| 5.6.3.3 | The solution shall ingest and correlate EIDO data objects, including audio, video, telematics, additional location reporting (ALR), and multimedia. |
| 5.6.3.4 | The solution shall support the migration of legacy MIS and historical call records into the analytics platform. |
| 5.6.3.5 | The solution shall implement automated data quality validation to detect missing, duplicate, late-arriving, conflicting, or malformed records across all ingested data sources. |
| 5.6.3.6 | The solution shall provide configurable data completeness and accuracy thresholds and shall flag analytics outputs that do not meet Customer-defined quality standards. |

| | |
|---|---|
| 5.6.3.7 | The solution shall reconcile discrepancies near real time between CHE, CAD, NGCS, and GIS data and shall provide visibility into which source was used for each analytic output. |
| 5.6.3.8 | The solution shall assign confidence or quality indicators to analytics results derived from multiple or conflicting data sources. |

| **5.6.4** | **Analytics Dashboards & Reporting** |
|---|---|
| 5.6.4.1 | The solution shall provide role-based dashboards and reports for PSAP users, supervisors, administrators, and executives. |
| 5.6.4.2 | Operational dashboards shall refresh in sixty (60) seconds or less. |
| 5.6.4.3 | The solution shall support multi-tenant dashboards with regional roll-ups and PSAP-level drill-down while maintaining data segregation. |
| 5.6.4.4 | The solution shall provide an interactive dashboard and report library. |
| 5.6.4.5 | The solution shall support scheduled report generation with automated delivery in PDF, Excel, and CSV formats. |
| 5.6.4.6 | Standard operational dashboards shall load within Customer-defined performance thresholds under normal operating conditions. |
| 5.6.4.7 | The solution shall support concurrent access by multiple users across multiple PSAPs without degradation of dashboard refresh rates or query performance. |
| 5.6.4.8 | The Respondent shall disclose tested performance limits, including maximum record volumes, concurrent users, and historical data depth. |

| **5.6.5** | **Analytics Custom and Ad-Hoc Analytics** |
|---|---|
| 5.6.5.1 | Authorized users shall be able to create custom ad-hoc reports and visualizations without Respondent involvement. |
| 5.6.5.2 | The solution shall support report versioning and change tracking. |
| 5.6.5.3 | The solution shall execute ad-hoc queries against five (5) or more years of historical data without requiring Respondent optimization or intervention. |
| 5.6.5.4 | The solution shall provide administrators with controls to limit query scope or resource utilization to prevent system degradation during peak operations. |

| **5.6.6** | **Analytics Historical Data and Retention** |
|---|---|
| 5.6.6.1 | The solution shall retain and support analysis of at least five (5) years of historical data. |
| 5.6.6.2 | The solution shall enforce Customer-defined retention, purge, and archival policies. |
| 5.6.6.3 | The solution shall normalize timestamps across all ingested systems using a Customer-approved authoritative time source. |
| 5.6.6.4 | The solution shall detect, log, and alert when source system timestamps deviate from the authoritative time source beyond a configurable threshold. |
| 5.6.6.5 | Analytics outputs and exports shall disclose time normalization logic where cross-system correlation is performed. |

| **5.6.7** | **Analytics Geospatial and Location Intelligence** |
|---|---|
| 5.6.7.1 | The solution shall provide geospatial analytics, including heatmaps, clustering, and trend analysis. |
| 5.6.7.2 | The solution shall support location accuracy, uncertainty, and z-axis analytics. |
| 5.6.7.3 | The solution shall correlate PIDF-LO, GIS, Emergency Call Routing Function (ECRF), and LVF data for analytics. |

| **5.6.8** | **Analytics and Advanced AI** |
|---|---|
| 5.6.8.1 | The solution shall provide AI-based forecasting for call volume, staffing, and incident trends. |
| 5.6.8.2 | The solution shall support predictive incident hotspot modeling. |
| 5.6.8.3 | The solution shall provide anomaly detection for call spikes, repeat callers, and system errors. |

| | |
|---|---|
| 5.6.8.4 | The solution shall provide AI-generated natural language summaries of trends and metrics. |
| 5.6.8.5 | The solution shall implement explainable AI with human oversight for verification. |
| 5.6.8.6 | The solution shall require customer approval for AI model and updates. |

| **5.6.9** | **Analytics Regulatory and Performance Analytics** |
|---|---|
| 5.6.9.1 | The solution shall provide automated NENA, FCC, and state regulatory reporting templates. |
| 5.6.9.2 | The solution shall track SLA compliance, MOS, latency, uptime, failover success, and routing resiliency. |
| 5.6.9.3 | The solution shall provide a Regional Performance and Resiliency Dashboard. |
| 5.6.9.4 | The solution shall support configurable analytics-driven alerts for SLA violations, call spikes, abnormal trends, and data ingestion failures. |
| 5.6.9.5 | Alerts shall be configurable by role and deliverable via dashboard notification, email, or API. |
| 5.6.9.6 | Predictive or AI-generated alerts shall be clearly identified and distinguishable from historical or real-time metrics. |

| **5.6.10** | **Baseline Report Categories** |
|---|---|
| 5.6.10.1 | The solution shall provide a baseline library of standard reports for NG9-1-1 operations, administration, analytics, and regulatory compliance. |
| 5.6.10.2 | The solution shall provide baseline reports for call handling and operational analysis, including call volumes, answer times, abandoned calls, transfers, and call outcomes. |
| 5.6.10.3 | The solution shall provide baseline staffing and workforce reports analyzing call load versus staffing levels, workload distribution, and staffing forecasts. |
| 5.6.10.4 | The solution shall provide baseline CAD and incident reports including incident volumes, response times, and multi-agency activity. |
| 5.6.10.5 | The solution shall provide baseline GIS and location analytics reports including call density, hotspot analysis, and location accuracy trends. |
| 5.6.10.6 | The solution shall provide baseline text to 9-1-1, RTT, and multimedia analytics reports. |
| 5.6.10.7 | The solution shall provide baseline system performance and SLA compliance reports. |
| 5.6.10.8 | The solution shall provide baseline regulatory and compliance reports supporting NENA, FCC, state, CJIS, and public-records requirements. |
| 5.6.10.9 | The solution shall allow authorized users to modify baseline reports and create new custom reports without vendor intervention. |
| 5.6.10.10 | The Respondent shall identify which baseline reports are delivered out-of-the-box and which require configuration. |

| **5.6.11** | **Mapping Data Persistence** |
|---|---|
| **5.6.11.1** | The solution shall persist dispatch mapping data within the authoritative call record. |
| 5.6.11.2 | The solution shall persist mapping data elements, including breadcrumbs, z-axis information, location accuracy, and acceptance events. |
| 5.6.11.3 | The solution shall make persisted mapping data available for analytics, scheduled reports, and exports. |
| 5.6.11.4 | The solution shall ensure that court-ready call records include all mapping-derived data. |
| 5.6.11.5 | The solution shall retain, audit, and timestamp all persisted mapping data. |
| 5.6.11.6 | The solution shall ensure that mapping data is not transient or view-only. |
| 5.6.11.7 | Mapping data persistence requirements shall apply solely to the storage, analysis, reporting, and evidentiary preservation of mapping-derived data and shall not require the analytics solution to provide operational mapping or dispatch functionality. |

| 5.6.12 | Other |
|---|---|
| 5.6.12.1 | The solution shall use a Customer-approved authoritative time source across all analytics, reports, alerts, and audit logs. |
| 5.6.12.2 | The solution shall provide user-accessible visibility into data lineage, source systems, transformations, and calculation logic used for analytics and reports. |
| 5.6.12.3 | The solution shall support legal hold functionality to suspend deletion or modification of records. |
| 5.6.12.4 | The solution shall flag incomplete, conflicting, or low-confidence data in analytics and shall disclose the underlying reason for the flag where available. |
| 5.6.12.5 | The solution shall maintain version history for regulatory and compliance reports. |
| 5.6.12.6 | The solution shall support reproduction of analytics results and regulatory reports using the same data, logic, and configuration in effect at the time the report was generated. |

| 5.6.13 | Call Counting, Reconciliation, and Audit Integrity |
|---|---|
| 5.6.13.1 | The solution shall implement Customer-approved, written definitions for all call volume metrics, including but not limited to "Total Calls." Definitions shall explicitly state prior to running reports to which call types are included or excluded (e.g., 9-1-1, administrative, abandoned, misdials, test calls, transferred-in/out calls, conference legs, callbacks, duplicate records). |
| 5.6.13.2 | The Respondent shall disclose all call-counting rules, assumptions, and edge-case handling used by the system and shall not rely on undocumented or proprietary logic to calculate totals. |
| 5.6.13.3 | The solution shall record call activity using an immutable, append-only event model. Call records and associated events shall not be silently overwritten or retroactively altered once recorded. |
| 5.6.13.4 | Each call shall maintain a complete event history (e.g., creation, queue, answer, transfer, re-bid, disconnect, reclassification), with timestamps and source identifiers for each event. |
| 5.6.13.5 | The solution shall support "as-of" reporting that allows reports to be generated based on the data state as of a specified date and time, ensuring that the same report run multiple times produces the same results. |
| 5.6.13.6 | The solution shall support Customer-controlled report closeout or locking (e.g., daily or monthly) that freezes official call totals while preserving the ability to track subsequent late arriving data separately. |
| 5.6.13.7 | The solution shall explicitly identify late arriving or corrected call data that would impact previously closed reporting periods and shall quantify the effect of such data on call totals. |
| 5.6.13.8 | Reports shall display original totals, late adjustments, revised totals, and net deltas, along with the reason for each adjustment (e.g., delayed ingest, reconciliation, manual reclassification). |
| 5.6.13.9 | The solution shall identify a single authoritative system of record for call counts and define reconciliation rules when data is sourced from multiple systems (e.g., CHE, CAD, NGCS, MIS). |
| 5.6.13.10 | When discrepancies occur between systems, the solution shall provide traceable reconciliation logic, including matching keys, precedence rules, and resolution outcomes. |
| 5.6.13.11 | Users shall be able to drill down from any aggregate call metric to the individual call records and underlying events used to calculate that metric. |
| 5.6.13.12 | The solution shall provide audit visibility into any change in reported call totals, including what changed, when it changed, why it changed, and whether the change was system- or user-initiated. |
| 5.6.13.13 | All changes affecting call metrics shall be attributed to a specific system process or authorized user, with date/time stamps retained for audit purposes. |
| 5.6.13.14 | The Respondent shall provide documented test scenarios and expected outcomes demonstrating correct call counting for common PSAP conditions, including transfers, conferences, rebids, abandoned calls, callbacks, duplicate ANI/pANI records, and failover conditions. |
| 5.6.13.15 | Call-counting test scenarios shall be used during acceptance testing, and reported totals shall match the approved definitions and expected outcomes prior to system acceptance. |

## 5.7 Other Requirements

5.7.1 Objectives.

The Master Agreement awarded for TXShare may cover a variety of services. Each Customer that selects to utilize the Master Agreement will negotiate the specific services it needs into a Supplemental Agreement with a customized SOW for that Customer. All proposals must be made based on, and either meet or exceed, the requirements contained herein.

5.7.2 Service Area.

In preparing a proposal, you will designate what geographic region(s) will be served. You must specify, on the service area designation forms included with their proposal, the service areas that they are willing and able to provide goods and services to. A vendor does not have to propose to service the entire State of Texas, nor have to propose to service all fifty (50) states, to be considered for an award of a TXShare contract.

Service area designation forms are found in **Exhibit 3**.

5.7.3 Service Category Offer.

You should prepare a proposal that describes in detail the goods or services that you are proposing to provide. Proposals must demonstrate your capability to provide all or part of the requested services. A proposal will be evaluated only for the services it proposes.

## 5.8 Contract Type

If awarded, your proposal will result in a fixed price contract based on submitted pricing you propose. It is at your discretion to propose either unit pricing or a percentage discount off the list price for the goods or services you wish to offer. It is generally recommended that you propose a discount, however.

By signing this proposal, you certify that you have obtained and will continue to maintain during the entire term of this contract, all permits, approvals, or licenses necessary for lawful performance of its obligations under this contract.

## 5.9 Contract Term

A contract resulting from this RFP shall be effective for 24 months from the date of award. This contract will automatically renew for up to three (3) additional one-year periods, not to exceed five (5) years in total, unless earlier terminated as provided herein. NCTCOG reserves the right not to renew at its discretion.

## 5.10 Warranty/Guarantee

Please state in your proposal what warranty or guarantee may apply to the goods or services you are proposing.

## 5.11 Catalogs

Responding Offerors are requested to submit a proposal that will contain a schedule of goods or services line that would qualify under one or more of the Categories stated in Section 5.0 of these specifications. This schedule is commonly referred to as a "catalog".

Catalogs contain a range of items that are published in either an electronic or hard copy form and are modified from time to time to reflect internal and external changes in the vendor's marketplace. It is at the vendor's discretion to propose any limitations of the goods or services offered. A good or service offered must be listed in the catalog to be eligible for sale through a Category of the awarded contract.

Catalogs are to be submitted with the proposal and may be provided electronically using either a PDF document or web link. Use a spreadsheet or a searchable document containing the pricing information. A physically delivered hard copy of the catalog is NOT acceptable.

Catalogs may be priced with a percentage discount or a fixed unit price. Pricing may be one or multiple tiers of varying discounts based on purchase quantity.

## 5.12 Quality

It is expected that you have knowledge of all applicable industry standards, laws, and regulations and possess an ability to market and distribute the goods or services to members of the cooperative.

## 5.13 New Goods And Services

New goods and services may be added to the resulting contract(s) during the term of the contract by written amendment, to the extent that those goods or services are within the scope of this RFP and include, but will not be limited to, new services added to the manufacturer's list offerings, and services which reflect new technology and improved functionality. Service Categories or individual items of a fixed price nature are subject to review and approval of NCTCOG before addition to the contract. Individual items added to catalog awards do not require prior approval of NCTCOG.

## 5.14 All or Nothing Award

"All or nothing" proposals are not acceptable and will be rejected. You must be willing to accept a partial award for any combination of the Categories proposed at the discretion of NCTCOG.

NCTCOG may award contracts to multiple Offerors supplying comparable goods or services, also known as a multiple award schedule, or award the contract to a single vendor. NCTCOG's decision to make multiple awards or a single award will be based upon its sole discretion regarding the type of award that provides best value.

## 5.15 Pricing

When preparing your pricing, you should furnish pricing for each Category proposed and state "No Bid" for any Categories or sub-Categories you will not offer. NCTCOG will consider Categories individually and may make awards on each Category independently. NCTCOG reserves the right to select the proposal or proposals offering the most advantageous combination, with price and other evaluation criteria considered.

**NOTE: The final negotiated pricing (or discount) will be incorporated into the Master Services Agreement with the awarded vendor(s). The pricing information provided in your proposal will be public information and will not be accepted marked as proprietary or confidential.**

5.15.1 Catalog Pricing

There are two types of pricing that may be proposed for your catalog:

- Discount – Responding Offerors are requested to submit a proposal that will contain specific goods or services that would qualify under the Categories listed. A minimum percentage discount is to be stated for each Category. This is commonly referred to as "discount pricing". This is the recommended method.

  The catalog offering a percentage discount should identify which Category of goods or services are covered by the catalog and the corresponding minimum percentage discounts that apply. The discounts may be broken down by category and quantity, as well as by subcategory or tier (to the extent of the proposer's choosing). The Proposer may be creative in the percentage tier discounts to the extent deemed appropriate.

A link to the schedule of list pricing for all catalog items must be provided with the initial contract during execution, and whenever the list pricing is updated. By providing the current list pricing, a potential Customer can determine the maximum cost for each item by multiplying the contractually awarded minimum percentage discount times the current published list price. The current published list price will be posted on the awarded Contractor's landing page on the TXShare website.

Changes to a percentage discount catalog that add, modify, or delete items during the term of the contract are allowed at any time and without prior approval by NCTCOG. However, the minimum percentage discount list price is fixed and may only change through execution of a contract amendment. The awarded Contractor however does have the option to allow a greater percentage discount when negotiating a purchase with the Customer.

A discount percentage off of list is considered to be a minimum discount, so the awarded Contractor is free to offer greater percentage discounts to a Customer as part of a purchase negotiation. A zero discount off catalog proposal is acceptable but may put the Contractor at a disadvantage when the Customer is comparing prices among competing Contractors. The Contractor may lower the unit price or increase the minimum discount percentage to be more competitive in a particular situation.

It is recommended that when offering a wide variety of goods and services that you propose a catalog percentage discount for all items in that Category (except any specific items specifically stated as excluded). Discount pricing also negates the need for submitting a request to amend unit prices every time there is a price increase for the good or service, as the contract will be awarded for the percentage discount and not for a specific unit price.

Any goods or services that <u>are not</u> specifically listed in the awarded Category catalog is ineligible to be sold under the contract except under Category "Optional Ancillary Goods and Services". These "goods or services not specifically listed" items, which are priced at a discount off of list price, may be only sold in companion with other goods and services specifically stated in the catalog under one of the other Categories. Goods or services that <u>are</u> listed under any Category, including Optional Ancillary Goods and Services, may be sold as stand-alone items.

Note: As previously stated, percentage discounts from list price are allowed but a markup percentage from cost is <u>not</u>, as this method is not allowable for purchases made via Federal grant money. Prices stated as a markup from cost are a cause for disqualification of those portions of your proposal.

Note: You may stipulate different discounts off different products or types of service (subcategories) within each Category, provided you clearly indicates how the different discounts apply to which goods or service subcategories.

- <u>Unit Pricing</u> **-** Responding Offerors are requested to submit a proposal that will contain specific stated goods or services that would qualify under the Category. Each item on the schedule has a stated fixed price per unit. This is commonly referred to as "unit pricing". All items offered should identify which Category of goods or services they are being offered under and a detailed schedule should be prepared listing the product item description, packaging size, unit of measure, and unit price.

  Changes may not be made to a unit pricing catalog to add, modify or delete items or to the unit pricing itself without execution of a written contract amendment. Therefore, any changes to the catalog goods or services that the Contractor desires must be submitted in writing to NCTCOG.

Unit prices may only be increased by written request and may be subject to acceptance by NCTCOG through execution of a contract amendment.

Any good or service not specifically listed on the awarded unit price catalog is ineligible under the contract except under Category "Optional Ancillary Goods and Services". These optional items, which are priced as a discount off of list price, may be only sold in companion with other scheduled goods and services specifically stated in the catalog under one of the other Categories. The total dollar value of these Optional Goods and Services category items may not exceed 25% of the order to be placed.

5.15.2 General Proposal Information

You must clearly identify which Category your pricing submittal applies to.

You have the option (but are not required) to propose ancillary optional goods or services. Examples are similar product lines, inside delivery, set up, installation, maintenance agreements, travel costs, and other similar goods and services that are not specifically covered by any of the other PRICING CATEGORIES listed in the RFP. Please provide adequate information explaining what the ancillary good or service consists of.

Any good and or service that your business sells, and reasonably meets one of the category descriptions of this RFP, may be proposed. However, they all require pricing by either unit price or discount from list in the proposal. The list pricing may be by a schedule attached to your proposal or by a weblink to your business catalog. The pricing information, including link, are to be attached to the Price Sheet included in this RFP.

NOTE: Only goods or services categories that have pricing submitted in the proposal (either by unit cost or percentage discount off of list) are eligible for purchase through a contract award. You may propose pricing in a manner that works best for you to prepare your customized quotes to customers, but the pricing must be stated in such a manner that must be capable of audit by the customer.

- For example, if you propose a discount off list, then your current list price card for the items proposed must be made available so that the customer can calculate the contract price. Such would mean if you were proposing "10% discount off list price of tables", then you must provide with your proposal the current list price for tables offered under the contract.

5.15.3 Exhibit 1 Categories Offered – All bidders must complete this form to indicate which categories whey are offering in their proposal. Check the appropriate box. If you are offering an "Other Ancillary Good or Service", you must list those goods and services under this Category in order for the goods or services to be considered for award. Failure by the responding vendor to submit the clarifications by the deadline requested may result in disqualification of the proposal.

Note that not all RFPs will contain an Exhibit Price Sheet.

5.15.4 Market Basket - For Evaluation Purposes Only (If required).

**FOR EVALUATION PURPOSES ONLY**: Respondents are asked to fill out and return a copy of the Sample Market Basket Pricing Form, included as **Exhibit 2** in this RFP package. This item is used to evaluate a Respondent's 'best value' as opposed to raw percentage discounts, and is what is used to score your proposed pricing. This item will not be considered or used beyond evaluation purposes. Respondents are not required to fill out the entirety of the form – e.g., if a Respondent does not offer all of the items listed, they are asked to only fill out those that they do provide.

**Responses are encouraged from vendors who can only provide a handful of products. Respondents are not expected to be able to provide the entirety of the desired goods, though are welcome to if they are able.**

5.15.5 Price Escalation/De-escalation**.**

The unit pricing (or discount percentage) proposed by the Offeror shall be of a fixed price nature for the first six (6) months of the contract. Escalation requests may be made no more than every ninety (90) days and are subject to mutual written amendment to the contract between NCTCOG and the contractor. It is the responsibility of the contractor to petition NCTCOG changes to the pricing structure. The awarded contractor must provide upon request such supporting documentation as TXShare may require that justifies the requested price escalation.

A price change (based on the Bureau of Labor Statistics, Consumer Price Index escalation) may be considered. Price changes may not exceed the most recent 12-month CPI-U table. Request for increases must be submitted in writing for consideration. Should the price change be granted and NCTCOG accepts, a written amendment will be executed.

Price decreases (or discount percentage increase) may be made at any time and without written agreement. Further, the awarded vendor may negotiate more favorable pricing terms with the individual customer based on quantity or other conditions of purchase without seeking approval from NCTCOG. Change to unit prices in a contract must be approved via mutual execution of an amendment to the contract. In the event of price decreases, an executed amendment is not required. If applicable, a copy of, or link to, the vendor's current pricelist should be submitted with the Proposal.

5.15.6 Sales Tax & Freight.

Do not include sales tax in proposal pricing. Nearly all Customers will be tax exempt. Freight/shipping cost should be addressed in your pricing. There is full flexibility on the vendor's behalf as to whether these costs are included in the price, or an additional charge to be determined at the time of the negotiation between the Contractor and Customer. However, this must be stated up front at the time of the submission of the proposal. Failure to state the method in the proposal will result in a default assumption of "additional charge" for freight/shipping costs when evaluating the proposal.

## SECTION 6: HOW TO SUBMIT YOUR PROPOSAL

### 6.0 INSTRUCTIONS FOR RESPONDENTS

Please provide a written response regarding ability to meet each requirement as outlined in the Specifications (Section 5). Include any additional pertinent information on how your proposed solution meets each requirement. Provide any pertinent additional functionality and/or services not outlined in the Scope of Work that you wish to offer.

**Important Note: Your proposal shall consist of your responses to the Required Response Information outlined below.**

**Required Response Information**

Each section of information should be ***clearly defined*** using the following section or heading titles:

1. ***Certificate of Offeror and Statement of Understanding***

   The initial submission pages of your proposal will consist of:

   1. Completed Cover Page with addenda acknowledgment, if applicable (page 2 of this solicitation document)
   2. A brief statement demonstrating the respondent's understanding of the scope of work and/or the deliverables requested in this solicitation.

2. ***References***

   Include at least four (4) recent references for customers (preferably public agencies) for whom you have provided services similar to those requested in this solicitation within the last five (5) years. Please include the organization's name (if applicable), contact person, phone number, and email address for each reference. NCTCOG reserves the right to contact or visit any of the respondents' current and/or past customers to evaluate the level of performance and customer satisfaction.

3. ***Project-Related Experience and Qualifications***

   Proposals will be evaluated based on the respondents' experience in performing the requested scope of work and providing the required goods and services.

   Respondents shall provide a comprehensive overview of their organization's capabilities, experience, and expertise in delivering Next Generation 9-1-1 (NG9-1-1) Call Handling Systems and related functional elements. Emphasis should be placed on relevant past projects, particularly those involving public sector entities or Emergency Communications Centers (ECCs). Include:

   **a. Organization's Capabilities and Experience**

   Provide a detailed description of your organization's capabilities and experience in delivering the requested service category(ies).

   **b. Relevant Past Projects**

   Provide examples of past projects that demonstrate your organization's experience and success in delivering the requested service category(ies), with particular emphasis on successful engagements with ECCs. For each project, include the following information:

   - Project Description: A brief overview of the project, including objectives, scope, and outcomes.
   - Client: The name of the public sector entity or other organization served.
   - Technologies Used: The technologies and tools implemented as part of the project.
   - Results: The impact and benefits realized by the client as a result of the solution.

**c. Background and Years in Business**

Provide a brief overview of your organization, including:

- History: A summary of the organization's history and evolution.
- Years in Business: The number of years the organization has been in operation, including specific experience providing NG9-1-1 Call Handling Systems and associated functional elements.

If applicable, identify any subcontractors or third-party services that are utilized in the performance of fulfilling this RFP. Provide a general explanation and chart which specifies project leadership and reporting responsibilities, and how the team will interface with NCTCOG and Participating Entities' project management and team personnel.

**4. *Technical Proposal***

To qualify for consideration, vendors must complete responses to items listed in the following. These documents serve as a critical component of the evaluation process.

- **Attachment A** –NCT911 Narrative Support of NG911Functional Elements
- **Attachment B** - Workbook NG9-1-1 Functional Elements Supporting CHE, Data Analytics, Dispatch Mapping, and Ancillary Services

Mandatory Sections - Respondent is required to fully complete the following sections of the RFP Workbook:

- **Tab 5.2 – Industry Standards**
- **Tab 5.3 – Technical and General Requirements**

o Service Category - For the following service categories, vendors are only obligated to complete the sections that correspond to the specific services for which they seek to be considered:

- **Tab 5.4 – Service Category #1: Standards-Based NG9-1-1 Call Handling System (CHE)**
- **Tab 5.5 – Service Category #2: Dispatch Mapping Solution for NG9-1-1**
- **Tab 5.6 – Service Category #3: Data Analytics Solution for NG9-1-1**

Failure to complete the mandatory sections or the relevant service category sections may result in disqualification from the evaluation process.

Failure to provide written response to items indicated in this section will be interpreted by NCTCOG as an *inability* by the firm to provide the requested product, service or function.

**5. *Value-Added Capabilities and Innovations***

Respondents are invited to propose value-added functionality, services, or approaches that are not explicitly identified in the Scope of Work but may enhance overall outcomes, efficiency, performance, or long-term value. Such proposals shall complement, and not replace, the required solution.

Value-added offerings may include innovative features, best practices, optional services, or insights based on prior experience with similar implementations. Responses should clearly describe the benefit of each item and its relevance to the proposed solution.

***6. Pricing***

Respondents should furnish a proposal that specifies pricing for the services they propose. For more information, please refer to **Exhibit 1**. Points will be awarded on the basis of the overall cost effectiveness and clarity in identifying/explaining costs.

**7. *Exhibits 1 & 3***

- Please upload the completed Exhibit 1: Categories Offered and Pricing Proposal (pg. 106)

- Please upload the completed Exhibit 3: Service Designation Areas (pg. 108-110)

8. ***Cooperative Contracts***

List any cooperative purchasing programs or consortiums in which your organization has been an awarded vendor, currently or in the past. Include the following:

- Cooperative Name
- Contract Scope
- Contract Duration

9. ***NCTCOG/TXShare RFP Attestations (I-XII)***

Please upload the completed and signed RFP Attestations documents in the space provided in BidNet. All attestations must be included with your proposal; failure to do so may result in disqualification as non-responsive. If an attestation item does not apply, mark it as **"Not Applicable"**, sign the document, and submit it with your proposal.

## APPENDIX A: SERVICE LEVEL FRAMEWORK AND COMPONENT SLAS

This Appendix defines the Service Level Agreements (SLA) and Service Level Requirements (SLR) for three independently procured solution components:

- Section A – Call Handling Equipment (CHE)
- Section B – Dispatch Mapping
- Section C – MIS / Data Analytics

Each section is contractually independent in enforcement and remedies, while sharing a common framework for governance, measurement, and reporting.

## A.0 Common SLA / SLR Framework (Applies to All Sections)

### A.0.1 Applicability

Unless otherwise stated, the terms, definitions, incident priorities, response times, repair times, escalation intervals, reporting requirements, and remedies defined in this Appendix apply equally to Sections A, B, and C.

### A.0.2 Measurement Period

All SLA metrics shall be measured on a rolling monthly basis and reported via a secure dashboard.

### A.0.3 Support Availability

- 24/7/365 support, North America based

### A.0.4 Incident Priority Levels

| Priority | Definition |
|---|---|
| **Priority 1 – Critical** | Complete or near-complete loss of service impacting emergency operations |
| **Priority 2 – Major** | Significant degradation of service |
| **Priority 3 – Minor** | Partial loss with workaround |
| **Priority 4 – Non-Service Impacting** | Cosmetic or scheduled changes |

### A.0.5 Response and Repair Targets

| Priority | Response Time | Repair Target |
|---|---|---|
| P1 | 15 minutes | 2 hours |
| P2 | 30 minutes | 4 hours |
| P3 | 8 hours | 48 hours |
| P4 | Next business day | As agreed |

### A.0.6 Chronic Failure Clause

Repeated failure to meet the same SLR three times in six months or five times in twelve months constitutes Chronic SLA Failure and may result in corrective action or material breach.

# Section A – Call Handling Equipment (CHE)

## A.1 Scope

Applies to all CHE components including call processing, routing, media handling, failover, and inter-PSAP transfers.

## A.2 Service Level Requirements

| SLR ID | Metric | Objective |
|---|---|---|
| CHE-1 | Availability | 99.999% |
| CHE-2 | Call Continuity | No more than one outage ≥6 minutes per month |
| CHE-3 | Voice Quality (MOS) | ≥ 4.0 |
| CHE-4 | Failover | No call loss |
| CHE-5 | Incident Notification | ≤ 15 minutes |
| CHE-6 | Standards Compliance | ≤ 18 months from ratification |

## A.3 Remedies

Credits apply as service credits only and are capped at 25% monthly CHE fee.

# Section B – Dispatch Mapping

## B.1 Scope

Applies to all mapping, GIS, routing, z-axis visualization, and related integrations.

## B.2 Service Level Requirements

| SLR ID | Metric | Objective |
|---|---|---|
| MAP-1 | Availability | 99.95% |
| MAP-2 | Map Load Time | ≤ 2 seconds |
| MAP-3 | Location Update Latency | ≤ 5 seconds |
| MAP-4 | GIS Alignment | Authoritative alignment per Customer-approved sources |

| SLR ID | Metric | Objective |
|---|---|---|
| MAP-5 | Outage Notification | ≤ 15 minutes |
| MAP-6 | Offline Basemap | Available during outages |

### B.3 Remedies

Credits capped at 25% of monthly mapping fee.

## Section C – Data Analytics

### C.1 Scope

Applies to data ingestion, dashboards, reports, analytics availability, and historical access.

### C.2 Service Level Requirements

| SLR ID | Metric | Objective |
|---|---|---|
| DATA-1 | Availability | 99.9% |
| DATA-2 | Dashboard Refresh | ≤ 60 seconds |
| DATA-3 | Data Latency | ≤ 5 minutes |
| DATA-4 | Scheduled Reports | On time |
| DATA-5 | Historical Retention | ≥ 5 years |
| DATA-6 | Accuracy | No material inaccuracies per audit criteria |

### C.3 Remedies

Credits capped at 25% of monthly analytics fee.

## A.9 Independence of SLAs

Failure in one section does not excuse or offset obligations in another.

## A.10 AI Readiness (Non-Punitive)

AI features are excluded from financial remedies unless designated production-critical by Customer.

## A.11 Governance

Monthly SLA reviews and quarterly executive reviews.

**EXHIBIT 1: CATEGORIES OFFERED AND PRICING PROPOSAL**

**Select the categories you are offering in your proposal:**

☐ **Service Category #1:** Standards-Based NG9-1-1 Call Handling System (CHE)

☐ **Service Category #2:** Dispatch Mapping Solution for NG9-1-1

☐ **Service Category #3:** Data Analytics Solution for NG9-1-1

☐ **Service Category #4:** Ancillary Services for NG9-1-1

**Catalog Submission**

Responding Offerors must submit a current catalog for the goods or services proposed under each applicable category. Catalogs must be provided electronically, either as an excel document, PDF document or via a web link, and must include searchable pricing information. Hard copy catalogs will not be accepted.

Catalog pricing may include percentage discounts, fixed unit pricing, or tiered pricing based on quantity. Only goods or services listed in the submitted catalog will be eligible for sale under any awarded contract category.

**Catalog Submission Format – Check One:**

☐ Excel or PDF Catalog Attached
☐ Web Link to Catalog: _____

**Pricing Submission Requirements**
Respondents must provide a pricing model in accordance with the guidance in **Section 5.15**, clearly indicating whether the pricing is based on **Discount Pricing** or **Fixed Pricing**. Pricing must be clearly delineated for **Service Categories**.

**Include the completed Exhibit 1 form with your proposal as outlined in Section 6.**
Your pricing must be submitted within BidNet, clearly labeled as:

**"Exhibit 1 – Pricing"**

- Use as many pages as necessary for your pricing details.
- Ensure that **Exhibit 1 – Pricing** is distinct and separate from your proposal.
- Submit all pricing information in the provided Envelope in BidNet.

**Important Note**: This RFP is not tied to any specific project at this time. The purpose is to secure pricing for potential future use by public sector entities. Respondents are encouraged to provide pricing models that are as descriptive and flexible as possible to accommodate the varied needs of potential users.

## EXHIBIT 2: SAMPLE MARKET BASKET FORM

A Sample Market Basket Form is not required for this RFP.

## EXHIBIT 3: SERVICE DESIGNATION AREAS

| | Texas Service Area Designation or Identification | | |
|---|---|---|---|
| **Proposing Firm Name:** | | | |
| **Notes:** | **Indicate in the appropriate box whether you are proposing to service the entire state of Texas.** | | |
| | Will service the entire state of Texas | Will not service the entire state of Texas | |
| | ☐ | ☐ | |
| | | | |
| | **If you are not proposing to service the entire state of Texas, designate on the form below the regions that you are proposing to provide goods and/or services to. By designating a region or regions, you are certifying that you are willing and able to provide the proposed goods and services.** | | |
| **Item** | **Region** | **Metropolitan Statistical Areas** | **Designated Service Area** |
| 1. | North Central Texas | 16 counties in the Dallas-Fort Worth Metropolitan area | |
| 2. | High Plains | Amarillo<br>Lubbock | |
| 3. | Northwest | Abilene<br>Wichita Falls | |
| 4. | Upper East | Longview<br>Texarkana, TX-AR Metro Area<br>Tyler | |
| 5. | Southeast | Beaumont-Port Arthur | |
| 6. | Gulf Coast | Houston-The Woodlands-Sugar Land | |
| 7. | Central Texas | College Station-Bryan<br>Killeen-Temple<br>Waco | |
| 8. | Capital Texas | Austin-Round Rock | |
| 9. | Alamo | San Antonio-New Braunfels<br>Victoria | |
| 10. | South Texas | Brownsville-Harlingen<br>Corpus Christi<br>Laredo<br>McAllen-Edinburg-Mission | |
| 11. | West Texas | Midland<br>Odessa<br>San Angelo | |
| 12. | Upper Rio Grande | El Paso | |

(Exhibit 3 continued on next page)

(Exhibit 3 continued)

| | Nationwide Service Area Designation or Identification Form | | |
|---|---|---|---|
| **Proposing Firm Name:** | | | |
| **Notes:** | **Indicate in the appropriate box whether you are proposing to provide service to all Fifty (50) States.** | | |
| | Will service all fifty (50) states | Will not service fifty (50) states | |
| | ☐ | ☐ | |
| | | | |
| | **If you are not proposing to service to all fifty (50) states, then designate on the form below the states that you will provide service to. By designating a state or states, you are certifying that you are willing and able to provide the proposed goods and services in those states.**<br><br>**If you are only proposing to service a specific region, metropolitan statistical area (MSA), or City in a State, then indicate as such in the appropriate column box.** | | |

| **Item** | **State** | **Region/MSA/City (write "ALL" if proposing to service entire state)** | **Designated as a Service Area** |
|---|---|---|---|
| 1. | Alabama | | |
| 2. | Alaska | | |
| 3. | Arizona | | |
| 4. | Arkansas | | |
| 5. | California | | |
| 6. | Colorado | | |
| 7. | Connecticut | | |
| 8. | Delaware | | |
| 9. | Florida | | |
| 10. | Georgia | | |
| 11. | Hawaii | | |
| 12. | Idaho | | |
| 13. | Illinois | | |
| 14. | Indiana | | |
| 15. | Iowa | | |
| 16. | Kansas | | |
| 17. | Kentucky | | |
| 18. | Louisiana | | |
| 19. | Maine | | |

| | | | |
|---|---|---|---|
| 20. | Maryland | | |
| 21. | Massachusetts | | |
| 22. | Michigan | | |
| 23. | Minnesota | | |
| 24. | Mississippi | | |
| 25. | Missouri | | |
| 26. | Montana | | |
| 27. | Nebraska | | |
| 28. | Nevada | | |
| 29. | New Hampshire | | |
| 30. | New Jersey | | |
| 31. | New Mexico | | |
| 32. | New York | | |
| 33. | North Carolina | | |
| 34. | North Dakota | | |
| 35. | Ohio | | |
| 36. | Oregon | | |
| 37. | Oklahoma | | |
| 38. | Pennsylvania | | |
| 39. | Rhode Island | | |
| 40. | South Carolina | | |
| 41. | South Dakota | | |
| 42. | Tennessee | | |
| 43. | Texas | | |
| 44. | Utah | | |
| 45. | Vermont | | |
| 46. | Virginia | | |
| 47. | Washington | | |
| 48. | West Virginia | | |
| 49. | Wisconsin | | |
| 50. | Wyoming | | |

End of Exhibit 3