# Attachment F – ESInet and NGCS Technical Requirements

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

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

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

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

**CONTENTS**

### 1.1 ESInet Architecture

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Has diverse entrance facilities for core sites and call-answering endpoints | | | |
| 2. Has no single points of failure, including "last mile" | | | |
| 3. Uses open standards | | | |
| 4. Supports IPv4 and iPv6 dual protocol stacks | | | |
| 5. Supports Border Gateway Protocol (BGP) utilizing Bidirectional Forwarding Detection | | | |
| 6. Supports multicast routing and switching | | | |
| 7. Supports quality of service (QoS) marking using Differentiated Service Code Point (DSCP) | | | |
| 8. Shall have a network traffic convergence of less than 54 milliseconds (ms) | | | |
| 9. Maintains a Mean Opinion Score (MOS) of 4.0 or better at the handoff to the CHE | | | |
| 10. Is scalable to support bandwidth growth by 50 percent | | | |
| 11. Shall interface with other i3-compliant ESInets to facilitate ESInet-to-ESInet transfers retaining standard data | | | |
| 12. Provides redundant in-LATA POI[1] for originating service providers | | | |
| 13. Failure of any single instance of a hardware or software element, or physical connection, shall not negatively impact overall solution performance | | | |
| 14. All network-connected elements must support at least two redundant network interfaces | | | |
| 15. All powered devices must include a minimum of two redundant power supplies (each of which must be able to power the device alone, and which would be connected to separate circuits) OR be connected to a power-transfer device that allows a single power supply to be connected to two isolated | | | |

[1] Local access and transport area; point of interconnection.

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| power sources (i.e., circuits) with automatic, uninterrupted failover, in the event the primary circuit fails | | | |

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

### 1.2 Security

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Provide a completed NENA NG-SEC compliance matrix | | | |
| 2. Have a security plan (physical, logical, and network) | | | |
| 3. Perform proactive analysis of the network for vulnerabilities | | | |
| 4. Provide a defined continuity of operations (COOP) plan as well as a disaster recovery (DR) plan | | | |
| 5. Provide access reports from facilities down to the individual device level | | | |
| 6. Require multifactor authentication for any access to externally accessible portals, user interfaces (UIs), etc. (Policy Routing Function [PRF] portal, reporting portal, system dashboards, etc.) | | | |
| 7. Have a formal change-control process documented with rollback procedure and management approvals that is strictly followed by technicians (in order to prevent unnecessary and/or uncontrolled maintenance from negatively impacting the 9-1-1 system) | | | |

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

### 1.3 Documentation

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Proposed network design (transitional and end state) | | | |
| 2. As-built documentation prior to the system final acceptance | | | |
| 3. Network interface specifications for ESInets | | | |
| 4. Network interface specifications for CHE | | | |
| 5. User's guide for all user-accessible solution elements | | | |
| 6. Detailed network design drawings reflecting the physical and virtual IP paths provided to each PSAP, including what is provided by subcontracted last-mile providers and/or resellers, prior to beginning system testing | | | |

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

### 1.4 Facilities

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. All power sources must be redundant and diverse (i.e., at least two separate circuits) with an uninterruptible power supply (UPS) system and generator backup for a minimum of 24 hours | | | |
| 2. Voice and data circuits delivered via diverse entrances into facilities | | | |
| 3. Voice and data circuits delivered from diverse providers | | | |
| 4. Secured rack space | | | |
| 5. Minimum Tier 3 rated | | | |
| 6. Hardened facilities that can withstand F5-category winds up to 318 miles per hour | | | |

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

### 1.5 Monitoring and Alarming

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Physical access monitoring and reporting | | | |
| 2. Automated network node monitoring and alarming | | | |
| 3. Integrated alarming and ticketing system | | | |
| 4. Ability to display network node status in a client-facing dashboard | | | |
| 5. User-definable notification levels and recipients, with text and email delivery options | | | |

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

### 1.6 Network Operations Center/Security Operations Center

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. 24 x 7 staffed network operations center (NOC)/security operations center (SOC) | | | |
| 2. Ability for users to submit tickets by phone, email, and direct ITSM[2] user access for incidents, problems, and changes | | | |
| 3. Perform outward notifications and updates of customer tickets through phone, email, and text | | | |
| 4. Have an executive dashboard with (near) real-time updates of tickets and network status | | | |
| 5. Comply with service level agreements (SLAs) for notification and ticket resolution | | | |
| 6. Reason for outage (RFO) reports and regulatory compliance according to Federal Communications Commission (FCC) standards | | | |
| 7. Preliminary RFO reports are due to GCRECD within five business days; final root-cause analysis within 15 calendar days | | | |
| 8. Media contact for any outage or service failure | | | |
| 9. Government and regulatory contact for any outage or service failure | | | |
| 10. COOP plan | | | |
| 11. Access to technical staff for escalations | | | |

[2] IT service management.

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 12. Compliance with Statement on Standards for Attestation Engagements Number 16 (SSAE 16) | | | |
| 13. Support of eBonding in the ITSM platform | | | |
| 14. Support of third-party NOC/SOC integrations | | | |
| 15. Have established escalation procedures | | | |
| 16. All NOC/SOC access is United States (U.S.) based; no "offshore" remote access for system administration | | | |

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

### 1.7 NGCS Functional Elements

The Respondent shall provide an NGCS solution that includes (at a minimum) the functional elements in the table below. Each element must meet or exceed NENA STA - 010.3b-2021:

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Legacy Network Gateway (LNG)/Legacy Selective Router Gateway (LSRG)/Legacy PSAP Gateway (LPG) | | | |
| 2. Border Control Function (BCF) | | | |
| 3. Emergency Services Routing Proxy (ESRP) | | | |
| 4. Policy Routing Function (PRF) | | | |
| 5. Emergency Call Routing Function (ECRF) | | | |
| 6. Location Validation Function (LVF) | | | |
| 7. Spatial Interface (SI) | | | |
| 8. Location Database (LDB) | | | |
| 9. Network Time Protocol and Time Source | | | |

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

### 1.8 OSP and Selective Router Migrations

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Certificate to operate as a CLEC[3] in the state of Texas | | | |
| 2. Integration of all OSP connectivity for wireline, wireless, and voice over IP (VoIP) traffic, as well as multi-line telephone systems (MLTS) | | | |
| 3. Coordinate with GCRECD to obtain letters of authority/agency | | | |
| 4. Establish interconnection and commercial agreements, and trunking | | | |
| 5. Provide interconnection document (ICD) for all OSP, CHE, and other third-party providers requiring ESInet connectivity | | | |
| 6. Coordinate with all telecommunications providers and manage circuit order processes to include testing and integration | | | |
| 7. Describe the process for analyzing current trunk engineering for 9-1-1 traffic, and validating any trunk rebalancing for public-safety-grade service | | | |
| 8. Manage all adds, moves, changes, and deletions of connections to OSPs, both TDM[4] and IP-based, monitor these connections, and proactively work with the respective OSPs to resolve problems as they occur | | | |
| 9. Coordinate and execute connectivity to all neighboring ESInets that require direct transfer capabilities; the list of required ESInets is to be determined solely by GCRECD | | | |
| 10. Coordinate and execute connectivity to neighboring ESInets to support transfers to neighboring agencies not served by GCRECD's NG9-1-1 solution | | | |
| 11. Define and manage all processes associated with split-rate centers, local number portability, and national number portability | | | |
| 12. Support transition of both TDM and SIP ingress to the ESInet | | | |

[3] Competitive local exchange carrier.
[4] Time-division multiplexing.

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

### 1.9 ALI Transition

The Respondent shall provide the services below to support the transition from legacy ALI[5] to i3 functional elements.

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Master Street Address Guide (MSAG) conversion service | | | |
| 2. Service order input (SOI) process for subscriber records | | | |
| 3. Integration and provisioning for MLTS databases | | | |
| 4. pANI[6] provisioning and shell records management | | | |
| 5. Manage the transition to include coordination of all provider records from the legacy ALI database to the replacement LDB and any dual provisioning necessary during the transitional phases of the project | | | |
| 6. Provide reporting for all data within the LDB via a web-based tool | | | |

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

[5] Automatic location identification.
[6] Pseudo automatic number identification.

### 1.10 Text-to-9-1-1

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Support for Message Session Relay Protocol (MSRP) | | | |
| 2. Support for Real-Time Text (RTT) capability | | | |
| 3. Support for transcoding of Baudot tones to RTT | | | |
| 4. Support for interconnection to third-party text control centers (TCCs) | | | |
| 5. NGCS can provide policy-based routing on incoming text messages | | | |
| 6. Supports text transfers from PSAP to PSAP across the ESInet | | | |
| 7. Text transfers will include caller location | | | |

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

### 1.11 TCC

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. The Respondent has or contracts TCC capabilities currently | | | |
| 2. The Respondent will provide TCC functionality to GCRECD as part of their NGCS deployments | | | |
| 3. The Respondent or the Respondent's contracted TCC receives text messages and provides 9-1-1 routing for all major wireless OSPs today | | | |
| 4. Support for interconnection to third-party TCCs | | | |

*Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Provide a description of your TCC partnerships and NGCS routing integration for text. Respondents can utilize GCRECD's current TCC contract if required. Add additional lines as needed.*

### 1.12 Logging and Recording

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Support for EIDO[7] and IDX[8] (once ratified by NENA) | | | |
| 2. Discrepancy reporting | | | |
| 3. Logging and recording | | | |
| 4. Describe the ability to support early media | | | |
| 5. Alarm integration (e.g., integration through a third-party and/or ASAP) | | | |
| 6. On-demand dynamic reports from the reporting UI | | | |
| 7. Support for logging and reporting of all relevant i3 events (as defined in section '5.13 Logging Service' of the latest version of "*NENA Detailed Functional and Interface Standards for the NENA i3 Solution*", at the time of this writing NENA-STA-010.3b-2021) | | | |
| 8. Multitenant partitioning of logs and call data, allowing for partitioned reporting, based on role, PSAP, or agency | | | |
| 9. Support for entering call notes | | | |
| 10. System must support the following built-in reports:<br>a. Call reports by day/week/month (number of total calls, wireless/wireline/VoIP calls, abandoned calls, geospatially routed calls, policy routed calls, transferred calls, etc.)<br>b. SIP error reports (within the ESInet)<br>c. ECRF and LIS/LDB location queries and results | | | |

[7] Emergency incident data object.
[8] Incident data exchange.

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| d. ESRP/PRF routing reports (errors and successes)<br>e. Location discrepancy reports<br>f. Call volume and time-to-answer reports | | | |
| 11. Support for ad hoc reports by custom date/timestamp range, and creation of customized report templates | | | |
| 12. Support for automated report generation and distribution | | | |

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

### 1.13 PCA

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Shall follow *NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines* | | | |
| 2. Registered as or able to acquire certificates from a PCA-vetted Intermediate Certificate Authorities (ICA) | | | |
| 3. Credentialing plan/process for third-party entities to get PCA-approved certificates | | | |
| 4. Shall support Forest Guide and hierarchical ECRFs when integrated with state or adjacent NG9-1-1 solutions | | | |

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

### 1.14 NGCS Availability

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Solution must provide geo-redundant and locally redundant NGCS | | | |
| 2. Solution must be locally redundant at the hardware and software application layers | | | |
| 3. Solution must maintain 99.999 percent availability | | | |
| 4. Failure of any single instance of a hardware or software element instance or physical connection shall not negatively impact overall solution performance | | | |
| 5. All network-connected elements must support at least two redundant network interfaces | | | |
| 6. All powered devices must include a minimum of two redundant power supplies (each of which must be able to power the device alone, and which would be connected to separate circuits) OR be connected to a power-transfer device that allows a single power supply to be connected to two isolated power sources (i.e., circuits) with automatic, uninterrupted failover if the primary circuit fails. | | | |
| 7. Due to events with the global pandemic GCRECD seeks confirmation that any committed plan and/or schedule communicated within this response will be maintained regardless of "supply chain impacts" | | | |

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

### 1.15 Training

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. SI users' interface tools | | | |
| 2. Reporting and logging tools | | | |
| 3. Incident reporting and ticketing tools | | | |
| 4. Dashboards | | | |
| 5. Change-management requests, processes, and tools | | | |
| 6. PRF policy management | | | |
| 7. GIS tools and procedures | | | |
| 8. SOI update procedures | | | |
| 9. LVF procedures | | | |
| 10. Scheduling, class size, location, recording, personalization, multilingual, etc. (i.e., logistics) | | | |

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

### 1.16 Other Integrations

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Additional data repositories (ADR), Identity Searchable ADR (IS-ADR), and/or commercial third-party LIS | | | |
| 2. i3-compliant call-handling solutions | | | |

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 3. Integration of all OSP-provided locations and other media types determined by NENA STA - 010.3b-2021 for delivery to CHE | | | |

*Use this space to elaborate on the compliance responses to the requirements in the table above. Include any additional information (diagrams, graphs, screenshots, etc.) you think is needed to describe how your solution addresses these requirements. Include in your response solutions you have successfully tested and deployed with (e.g., alarm companies, CHE, etc.) Add additional lines as needed.*

### 1.17 SLAs

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. 24 x 7 NOC/SOC | | | |
| 2. Ability to submit incident and trouble tickets by phone, email, or direct UI to the ITSM system | | | |
| 3. Documented escalation processes, procedures, and personnel | | | |
| 4. Call-processing capacity capable of 100 percent of busy hour call traffic | | | |
| 5. Ability to grow call-processing capability by 50 percent over contract duration without service disruption | | | |
| 6. Appendix B outlines the SLAs and penalties associated with failure to meet the same | | | |

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

### 1.18 Documentation

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. As-built solution design documentation to include configured parameters and policy-routing flow-downs (planned design and actual implemented design) prior to acceptance test plan review and execution | | | |
| 2. Interface specifications for call-handling solution provider | | | |
| 3. Operations manuals for all tools and UIs | | | |
| 4. Training plan | | | |
| 5. Project implementation plan | | | |
| 6. Pre-cutover acceptance test plan (ATP) for core network | | | |
| 7. Pre-cutover ATP per PSAP | | | |
| 8. NENA NG-SEC compliance matrix | | | |
| 9. SI user documentation | | | |
| 10. Project staffing plan | | | |
| 11. NOC/SOC user guides including change-management processes | | | |

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

### 1.19 Service Validation

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Independent third-party validation of the solution's features and functionality | | | |
| 2. SIP messaging logs, call detail records CDRs), and/or call logs to verify compliance with contractual obligations shall be provided to an independent third party for validation at the customer's direction | | | |
| 3. Documentation of completed results from ATPs | | | |
| 4. List the call-handling solutions successfully tested and deployed with your solution | | | |

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

### 1.20 Personnel

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

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

### 1.21 GIS

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Leverage GCRECD's GIS data for geospatial routing of 9-1-1 calls, and responses to CHE LoST[9] queries for law enforcement, fire, and EMS[10] response agencies | | | |
| 2. Provide secondary quality assurance (QA) and coalescing of GIS data to identify any structural issues with the data (attributes, formatting, missing layers, etc.) as well as any gaps and overlaps | | | |
| 3. Provide a web interface and/or automated method to provision GCRECD's data to the SI and retrieve post-QA data for the use of maps and/or the computer-aided dispatch (CAD) system | | | |

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

[9] Location to Service Translation
[10] Emergency medical services

### 1.22 Tools

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Web interface tool for accessing the LDB to extract reports, view telephone number (TN), MSAG, and GIS data; correct discrepancy reports (DRs); add status notes; and view transaction history, as needed, to support subscriber validation processes | | | |
| 2. Web interface tool for viewing and submitting incident and change tickets | | | |
| 3. Online dashboard showing the network, device, and monitoring/alarm status | | | |
| 4. Web interface tool for viewing policy-routing configurations | | | |
| 5. Web interface tool to access CDRs, searchable by date/time stamp, call back number, etc. | | | |
| 6. Call trace application showing SIP messaging (INVITEs, REFERs, SIP errors, etc.) as well as HELD[11], LoST, and ADR queries and responses | | | |

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

[11] HTTP (Hypertext Transfer Protocol)-Enabled Location Delivery

### 1.23 Change Management

Respondent's change-management process must have the following:

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

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

### 1.24 Pre-Cutover Acceptance Testing and Criteria

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Confirmation and documentation of equipment configuration | | | |
| 2. Confirmation and documentation of control, monitoring, and alarm solutions | | | |
| 3. ATPs and documentation provided 15 business days prior to testing for review by all necessary parties, including the third party | | | |
| 4. Include a pre-cutover ATP that contains testing processes for all functional elements in the proposal | | | |
| 5. Show that the plan can be tracked and measured | | | |

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 6. Respondent's NGCS ATP will be executed on the software revision the Respondent plans for deployment | | | |
| 7. If during testing, GCRECD believes that a solution test fails, GCRECD will provide the selected Respondent with a written description of what test failed and why; GCRECD will identify an expected amount of time that will be allowed to resolve the problem | | | |
| 8. Respondent takes full responsibility to work any GCRECD determined failed or partially failed test to an acceptable conclusion by GCRECD | | | |
| 9. If software changes or patches are required on any functional elements due to issues discovered during testing, the selected Respondent agrees to perform validation testing again and provide the results to GCRECD for review | | | |

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

### 1.25 Cutover Coordination

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Must coordinate cutover activities with all service providers, GCRECD staff, and PSAP personnel; GCRECD will have final approval of all cutover schedules | | | |
| 2. A detailed cutover plan, along with coordination, conference calls, and supporting documentation, must be provided to all participating parties | | | |
| 3. GCRECD is responsible for review and approval of the cutover plan | | | |
| 4. Shall provide trained and capable technical and functional solution support, and the project manager shall be available and onsite the day of cutover | | | |

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 5. Respondent shall describe in its proposal how many of its staff will be available, and their areas of expertise | | | |

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

### 1.26 PSAP Acceptance Testing

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. PSAP acceptance testing is the execution of the approved pre-cutover test plan to confirm that the selected Respondent's solution operates as expected and that the PSAP is ready for cutover to the live NG9-1-1 system | | | |
| 2. PSAP acceptance testing will cover PSAP-specific requirements such as policy validation and transfer capabilities with all expected functionality fully operational such as location and ability to transfer text conversations | | | |
| 3. Contract deliverables must perform in compliance with all RFP and contract requirements | | | |
| 4. PSAP acceptance testing shall be completed no less than seven days nor more than 30 days before the PSAP is scheduled to cutover | | | |
| 5. The selected Respondent shall implement a change control freeze at the completion of each PSAP's acceptance testing, except in extreme cases, in order to prevent any system maintenance activities from breaking functionality or otherwise rendering the PSAP no longer ready to cutover | | | |

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

### 1.27 System Final Acceptance

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. System final acceptance cannot begin until all PSAPs have successfully cutover to the live NG9-1-1 system; the final acceptance period, 30 consecutive calendar days, must be sufficient to demonstrate the solution's performance and reliability | | | |
| 2. Contract deliverables must perform in compliance with all RFP and contract requirements throughout the acceptance period. If a failure to comply occurs: | | | |
| a. GCRECD will provide written notification to the selected Respondent | N/A | N/A | N/A |
| b. The selected Respondent shall remedy the non-compliance per the Service Levels and Service Management Performance Standard sections of the contract and provide written notification of the remedy to GCRECD | | | |
| c. The final acceptance period will restart upon GCRECD's written notification of acceptance of the remedy, or three business days, whichever is less | | | |
| d. This procedure continues until compliance over the final acceptance period is achieved, at which time the contract deliverables will be deemed fully accepted and the acceptance notice will be mutually executed | | | |
| e. GCRECD will provide a Notice of System Final Acceptance once the period is successfully completes | | | |

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

### 1.28 System Final Acceptance Fault Categories

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| The following fault categories are defined for use during the final acceptance process. All GCRECD detected faults will be documented, and the documentation will include a limited but reasonable time in which the fault is to be resolved by the selected Respondent. | | | |
| 1. Priority One Fault — A critical system fault that renders the solution even partially inoperable. These faults are unacceptable to GCRECD | | | |
| 2. Priority Two Fault — A major system fault that significantly reduces the solution's performance and ability to function; these faults are unacceptable to GCRECD and must be resolved before GCRECD will accept the solution | | | |
| 3. Priority Three Fault — A minor system fault that marginally affects system performance and functionality; these minor faults are operational in nature and only acceptable while in the final acceptance phase. These faults must be resolved before GCRECD will accept the solution | | | |
| 4. Priority Four Fault — A combination of minor system faults and items that are on the punch list; these are items that have minimal or no effect on system performance and functionality. These faults must have a mutually agreed resolution timeframe before GCRECD will accept the solution | | | |

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

### 1.29 Migration Plan

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Within 30 days of contract signing, the selected Respondent shall provide a detailed migration plan that shall include a full description of the methods and procedures that will be employed to ensure a non-service-affecting migration from the current environment to the new system | | | |
| 2. The selected Respondent shall provide a recommended transition considering the complexity of the regional environment | | | |
| 3. This transition plan will recommend 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 of the region's configuration | | | |
| 4. The migration plan shall include a fallback procedure to restore GCRECD to a premigration operational state in the event of a catastrophic failure | | | |

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

### 1.30 Software Release Management

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Describe the frequency of scheduled software releases and the decision-making processes involved in deciding what features and defect resolutions to include in a scheduled release | | | |
| 2. Maintenance releases and feature releases shall be provided to GCRECD at no cost while a maintenance agreement is in place | | | |
| 3. Describe the frequency of defect-resolution software releases and the decision-making processes involved in selecting which software defects to fix | | | |

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 4. Provide GCRECD read-only access to the Respondent's defect tracking system in order to track the progress of GCRECD's reported defect resolutions.<br><br>The selected Respondent shall provide user training to GCRECD staff, prior to GCRECD's final acceptance testing | | | |
| 5. Include in the proposal the procedure to manage and track changes made to the system. 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 GCRECD staff | | | |
| 6. Notify and coordinate scheduling with GCRECD whenever solution servicing requires onsite visits; notification shall occur no less than ten business days before the needed visit and scheduling shall be at the sole discretion of GCRECD | | | |
| 7. Provide release notes to GCRECD no less than ten business days prior to system upgrades or updates, clearly identifying any new functionality of which GCRECD may wish to take advantage | | | |
| 8. Request authorization from GCRECD no less than ten days prior to performing maintenance, upgrades, backups, restorations, or other system changes that may impact the performance or functionality of the system or service (depending on how the call-handling solution is procured). The only exception to this advance-notice requirement is in cases where an update or upgrade is immediately required to restore a failed or failing service or component | | | |

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

### 1.31 Project Management

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. The Respondent shall provide a high-level project plan and timeline that shows the entire project with its response | | | |
| 2. A task-oriented Gantt chart based on the project plan and created in Microsoft (MS) Project | | | |
| 3. The steps that will be followed so that no service interruptions occur | | | |
| 4. Examples of what should be included in the project plan, at a minimum: | | | |
| a. Data gathering | | | |
| b. GCRECD onsite testing | | | |
| c. Core component installation and testing | | | |
| d. ALI, format, and interface testing | | | |
| e. Comprehensive test and acceptance plan for all network connections verifying complete functionality with the CHE | | | |
| f. A more detailed project plan, timeline, and a Gantt chart created in MS Project, due to GCRECD within 30 days of contract signing | | | |
| g. Conduct a kickoff meeting at GCRECD within 30 days of contract signing | | | |
| 5. Provide a project manager | | | |

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

### 1.32 Progress Reports

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

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

### 1.33 GCRECD Unique Requirements

| Requirements: | Complies | Does Not Comply | Partially Complies |
|---|---|---|---|
| 1. Multitenant operation and support | | | |
| 2. Make-busy functionality, (e.g. abandon switch, web tools, etc.) | | | |
| 3. Ring-down functionality | | | |
| 4. Near-simultaneous conference and transfer | | | |
| 5. Conference with, transfer to, and alternate route to 7/10-digit numbers | | | |
| 6. Transition of all legacy services shall be the responsibility of the selected Respondent; as such the Respondent shall ensure migration of all legacy connections and associated costs are completed within 120 days of the NGCS system "go live" date | | | |
| 7. Issue service credits to offset any legacy costs not transitioned within 120 days of the NGCS "go live" date, effectively ensuring there is no "double billing" for legacy and NG9-1-1 costs | | | |

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