Cloud-Based 9-1-1 Call Handling System
Supplemental Narrative Statement

General System Requirements

- Is the cloud-based 911 Call Handling solution NG911-compliant and aligned with NENA i3 standards?
- Is the vendor/system authorized to connect to the State or a regional ESInet?
- Does the redundant cloud hosting environment utilize geographically diverse data centers? Provide specific details.
- Is the system architecture scalable to accommodate fluctuating call volumes?
- Are 24/7 monitoring and technical support services available?

Connectivity & Network Readiness

- Are there secure and redundant connection paths to the ESInet? Provide detailed specifications.
- Is a Network-to-Network Interface (NNI) configuration supported?
- Does the system utilize IP-based SIP trunking with TLS and SRTP encryption protocols?
- Are Public Safety Grade Service Level Agreements (SLAs) in place? Attach SLAs.
- Have all relevant IP addresses and DNS details been provided to the ESInet provider (AT&T, Allerium (Comtech), or INdigital)?

Call Handling Capabilities

- Can the cloud-based Call Handling System (CHE) receive SIP-based 911 calls with complete PIDF-LO location information?
- Is Real-Time Text (RTT) supported?
- Does the system provide TTY compatibility?
- Are transfer capabilities to and from adjacent PSAPs over the ESInet supported, including full metadata preservation?
- Are features such as call queuing, priority routing, and selective routing implemented?

Location & Data Handling

- Is the system integrated with a Location Information Server (LIS)?
- Can location data be displayed and acted upon in real time?
- Are logs and records of ALI, PIDF-LO, and routing decisions stored securely and in compliance with applicable standards?
- Does the CHE support NG911 multimedia data types such as video, images, telematics, and sensor data?

Interoperability Testing

- Has the cloud provider successfully completed test scenarios with the ESInet provider?
- Has end-to-end call flow—covering call origination, routing, handling, and transfer—been validated?
- Has the accurate receipt and preservation of SIP headers and metadata been confirmed? Provide test results and outcomes.

Security & Compliance

- Is the system compliant with CJIS security requirements and SOC 2 Type II certified?
- Does the system support end-to-end encryption for both voice and data using TLS 1.2 or higher?
- Are role-based access controls and system audit logs implemented?
- Is a cybersecurity incident response plan in place? Attach the plan.

Training & Documentation

- Provide a training plan for Telecommunicators and IT staff.
- Provide detailed documentation covering call flow, failover mechanisms, recovery processes, and maintenance schedules.
- Include Tier 1 and Tier 2 support contact information.
- Include escalation procedures and confirm they have been shared with the ESInet provider.

Go-Live Preparation

- Have test calls been scheduled and coordinated with the ESInet provider? Provide testing schedule.
- Has a cutover plan been developed and shared? Attach the plan.
- Is a backup call routing plan confirmed? Attach the plan.
- Provide a contingency plan for system failure or degraded performance.