



MOTOROLA SOLUTIONS

Proposal

Nebraska Public Service Commission

RFP for Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS)

RFP # 202691101

April 15, 2026

Motorola Connectivity, Inc. is a wholly owned subsidiary of Motorola Solutions Inc. This document is protected by copyright law and international treaties, and is the information of Motorola Connectivity, Inc. All trademarks, service marks, product names, brands, company names and logos appearing in this document are the property of their respective owners. VESTA® is a registered trademark of Motorola Connectivity, Inc.

MOTOROLA, MOTO, MOTOROLA, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2022 All rights reserved
PS-000123456

Motorola Solutions Connectivity, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

April 15th, 2026

Dave Sankey
State 911 Director
Nebraska Public Service Commission
1200 N Street, Suite 300
Lincoln, NE 68508

RE: Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) to Enable Statewide Delivery of Next Generation 911 (NG911) - RFP 202691101

Dear Mr. Sankey,

Motorola Solutions Connectivity, Inc. (Motorola) appreciates the opportunity to provide the Nebraska Public Service Commission ("Commission") our NENA i3 compliant solution in response to the Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) to Enable Statewide Delivery of Next Generation 911 (NG911) - RFP 202691101. Motorola has over 90 years of experience in public safety communications and is an industry leader of NG911 systems, with deployments ranging from large statewide systems to small jurisdictions. With over 20 years of experience in routing 9-1-1 calls, we have refined our implementation and support expertise to the highest standards. Our Next Generation 9-1-1 call routing service currently serves more than 53 million people across North America.

As a leader in NG9-1-1, Motorola is offering the Commission and its agencies a fully compliant solution that meets all of your technical requirements without exception. The following key advantages combine our decades of experience, technological innovation, and commitment to public safety excellence to transform your emergency response capabilities:

- Provide redundant and diverse ESInet as a service.
- Network Security Operations Center (NSOC): Public Safety NSOC staffed 24/7/365 with experts ready to begin troubleshooting immediately.
- A Customer Access Portal that will keep you connected to your system.
- Winner of the 2022 IJIS Thomas J. O'Reilly Innovation Award for the first live NG9-1-1 i3 Location-Based Call Routing implementation.
- Winner of the 2023 Frost & Sullivan North American Technology Innovation Leadership Award for NGCS.

Motorola values the relationships that we have built over the years with the State of Nebraska and local agencies and looks forward to the opportunity to expand our role as a primary NG9-1-1 service provider.

The Commission can feel confident in working with Motorola, given our extensive experience and reputation in public safety, our broad range of resources, and our financial stability.

Any questions the Commission has regarding this proposal can be directed to Brett Nommensen, Executive Account Manager Strategic Projects, at (847) 561-6686, brett.nommensen@motorolasolutions.com or Carlos Simmonds, NG9-1-1 Regional Manager at (936) 320-1035, carlos.simmonds@motorolasolutions.com

Our goal is to provide the Commission with the best products and services available in the 9-1-1 industry. We thank you for the opportunity to present our proposed solution, and we hope to strengthen our relationship by implementing this project.

Sincerely,



Travis Boettcher

CVP Software Sales

Motorola Solutions Connectivity, Inc.

Nebraska Public Service Commission

Emergency Services IP Network (ESInet)
and Next Generation Core Services (NGCS)

April 15, 2026



MOTOROLA SOLUTIONS



Understanding Nebraska's needs

The Nebraska Public Service Commission (“NPSC” or “the Commission”) has articulated its objective to design, implement, operate, and support a cost-effective statewide Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) solution. This initiative is designed to provide high availability, security, scalability, and interoperability for NG9-1-1 communications across the state.

Ensuring the safety of Nebraska's residents and visitors requires the deployment of a redundant and reliable end-to-end i3 NG9-1-1 service in partnership with an experienced and qualified provider. The primary goals for this new system include:

- Delivering a highly available, resilient ESInet and NGCS platform that meets applicable NG911 standards and the Commission's requirements.
- Enabling seamless interoperability among regions and PSAPs, with defined service levels and 24/7 operations and support.
- Providing a structured migration, testing, and cutover plan that minimizes risk and service disruption.
- Supplying performance monitoring, real-time reporting, and analytics to support operational oversight and continuous improvement.
- Ensuring security, privacy, and compliance aligned with applicable rules, with clear incident response and disaster recovery capabilities.

As an industry leader in NG9-1-1 solutions, Motorola Solutions can help the Commission meet its vision, including:

- A transition from the current solution to a fully managed NG9-1-1 i3 call routing and i3 data delivery platform
- A highly available and resilient solution that meets and exceeds applicable NG9-1-1 standards and state requirements which in turn will provide the greatest value for Nebraska agencies and citizens
- Significant reduction in call transfers, saving critical time in emergency response by more than 50%
- Minimal disruption to stakeholders during planning and implementation
- Optimized support for the future needs of NG9-1-1 operations

Motorola has the expertise to provide you with the NG9-1-1 call routing solution that the Commission requires. With decades of experience in NGCS technology and trusted public safety partnerships with customers throughout North America, Motorola can ensure the successful deployment of a service that will meet and exceed your expectations.



The Motorola difference

Motorola stands out as the only vendor fully capable of delivering unparalleled success for your project, leveraging our expertise as a leader in NG9-1-1 services. We provide location-based call routing from day one, a carrier-agnostic design, and an implementation strategy that minimizes disruption.

Key focus	Motorola Difference	Benefit to the Commission
Experience, qualifications, and project management	• 30+ years of successful 9-1-1 call routing deployments • Experienced project team, with deep PSAP expertise • Proven project management Institute methodologies	• We utilize rigorous standards to ensure your project stays on schedule and your budget remains intact. • Partner with a team dedicated to delivering high-availability, compliant infrastructure that serves as a foundation for your long-term success.
Solution design and compliance	• NENA i3-compliant, carrier-agnostic design featuring redundant ESInet, 100% location-based routing, and end-to-end Motorola support	• We build for i3 standards from day one, saving you the heavy costs of future retrofitting, mid-project change orders, and redundant cutovers. • Improved efficiency through reduced call transfer times • Enhanced service reliability with uninterrupted operation during carrier outages
Implementation, installation, migration	• Proven implementation plan has reduced the average cycle time from Contract Date to Go Live by ²/₃ • Emphasis on communications • Live project workbook for immediate up-to-date information on implementation status	• Our zero-disruption migration gets you off your unreliable current system and onto a stable platform without a second of downtime. • You get a “no-surprises” partnership with complete visibility into every milestone, decision, and metric.
Maintenance and support	• Dedicated Public Safety Network and Security Operations Center for support • Full transparency with the Customer Web Portal	• Proactive identification and resolution of issues, minimizing downtime and maximizing system reliability • On-demand visibility into your Call Routing Service performance

The following pages provide details into how our experience and our proposed solution meet or exceed the Commission's RFP requirements.



The right partner

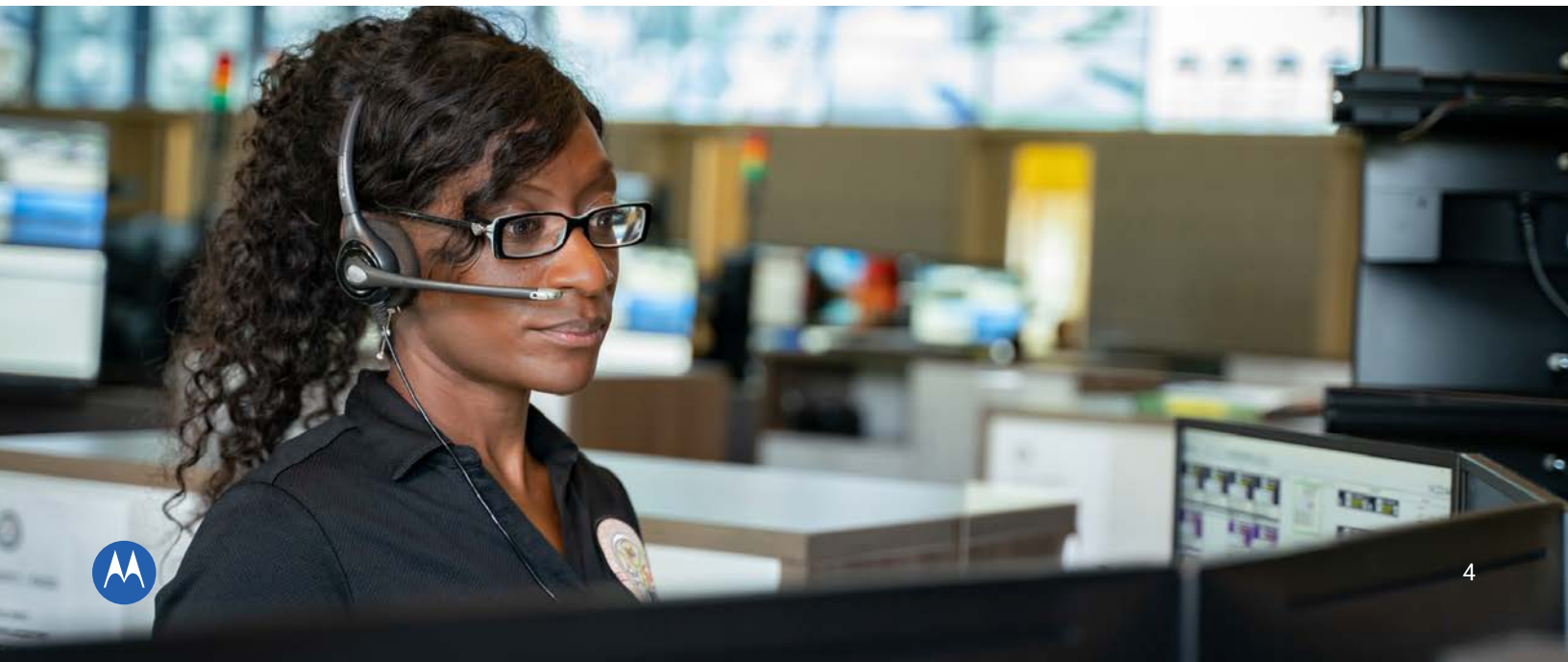
Experience, qualifications, and project management

Motorola is the ideal partner to modernize Nebraska's 9-1-1 system. Since 1928, Motorola has been focused on supporting public safety agencies with reliable communications that keep their communities safe. We're here to provide a lifeline. We not only build that lifeline – with missioncritical services, software, video, and analytics, backed by secure, resilient communications – we advance it every day through our commitment to innovation and through our strong partnerships with our customers.

We have long been an industry leader in call management solutions, including end-to-end Next Generation call routing and ESInet services.

With Motorola as your partner, The Commission can count on our expertise to deliver a successful deployment:

- **Unmatched value** – Our ESInet and i3 call routing platform are at the cutting edge of technology and are constantly evolving as new NG9-1-1 standards are introduced. We will keep you fully compliant and ready to tackle any emergency situation, providing the maximum value to Nebraska's agencies and citizens.
- **Seamless transition** – We include Originating Service Provider (OSP) migration as part of the standard project scope, in line with NENA i3 migration standards. You will be ready to take full advantage of NG9-1-1 call routing and benefits, including future video and multimedia options.
- **Minimal disruption** – We have implemented 9-1-1 call routing systems and upgrades throughout the country, at state-wide and county-wide levels, with no disruption to service. Our experience and expertise means we will deliver a disruption-free deployment for the Commission.
- **Unwavering support** – We will provide optimal support and transparency, both now and in the future, through our dedicated Public Safety Network and Security Operations Center (NSOC) and Customer Web Portal (CWP). Motorola is ready to help the Commission fulfill its vision for



Motorola's NGCS deployments

Serving

53+ million

people in the U.S. & Canada



State-wide / Province-wide

County or Regional deployment

Canadian Provinces

- Alberta
- British Columbia
- Saskatchewan

Florida

- Collier County
- Charlotte County
- Escambia County
- Lee County
- Manatee County
- Martin County
- Monroe County
- Okaloosa County
- Sarasota County
- St. Lucie County
- Sumter County
- Walton County

Idaho

- Statewide
- Ada County

Illinois

- City of Chicago

Kansas

- Johnson County*
- Leavenworth County*
- Miami County*
- Wyandotte County*

Louisiana

- Ascension Parish

Maryland

- Allegany County
- Anne Arundel County
- City of Baltimore
- Carroll County
- Frederick County
- Garrett County
- Howard County
- Prince George's County
- Washington County

Missouri

- Cass County*
- Clay County*
- Jackson County*
- Mercy Health Springfield Communities
- Platte County*
- Ray County*
- Greene County
- St. Charles County

* = Mid America Regional Council

Navajo Nation

- Arizona; New Mexico; Utah

Nevada

- North Las Vegas PD
- Las Vegas Metropolitan PD

New Mexico

- Statewide

Texas

- Brazos County ECD
- Brazos Valley Council of Govts
- City of Garland
- Central Texas Council of Govts
- Ector County ECD
- Galveston County ECD
- Golden Crescent Regional Planning Commission
- Harris County (Greater Houston)

New York

- New York City

Utah

- Statewide
- Hill Air Force Base

West Virginia

- Berkeley County
- Jefferson County

- Heart of Texas Council of Govts
- Henderson County 9-1-1 District
- Lubbock ECD
- McLennan County ECD
- Midland County ECD
- Montgomery County ECD
- Smith County 9-1-1 District
- Tarrant County 9-1-1 EAD



Our NG9-1-1 expertise and leadership

Our long-standing role as a leader in public safety technology enables Motorola to deliver a state-of-the-art system that will respond directly to the Commission's goals for this project.

Leadership in public safety

Motorola actively participates in organizations that lead the way for national standards, such as APCO and NENA, and we have been on committees to help define the standards for i3 compliance. **Our call routing solution is one of the industry's first cloud-based 9-1-1 call routing platforms that is NENA i3 compliant.**

Motorola participation in NENA

Employee current leader and member roles



Agency Systems Committee Document Review Work Group Member	Development Steering Council Co-Chair, Member	Document Management Work Group Member	EIDO Conveyance & JSON Work Group Member
GIS Data Model v3 Work Group Member	i3 Architecture Work Group Member	ICE 13 (and previous events) Member	ICE Steering Committee Member
Interface Specification Dev. Work Group Co-Chair	NG9-1-1 Interop Oversight Commission (NIOC) Representative	NG9-1-1 PSAP Systems Work Group Member	Supplemental Data Best Practices Work Group Member
International Committee Chair	Systems Security & Resiliency Committee Co-Chair	Transition to i3 PSAP Work Group Co-Chair	Utilization of GIS Data in NGCS Work Group Memeber

Motorola's commitment to NENA helps drive the advancement and implementation of next-generation 9-1-1 technologies and fosters a collaborative environment for improving emergency response across North America.

Motorola Solutions, Inc. Confidential Proprietary

Motorola's Call Routing Technology is Compliant with NENA's i3 Standards

“NENA's i3 standard is the foundation for interoperable, resilient next-generation 9-1-1 systems across the nation. It's a comprehensive, consensus-based, and commonly accepted open standard for next-generation 9-1-1, and we're happy to see providers like Motorola use it as a road map to more effectively connect the public to 9-1-1.”

– Brian Fontes, CEO of NENA



The right solution

Solution design and compliance

Motorola's solution for the Commission will provide a standards-based service that delivers accurate, seamless call routing and reduces call transfers. Our solution will remain compliant and up-to-date as standards evolve, ensuring that you are able to provide the best possible service to your community for years to come.

Network-agnostic ESInet

Our NG9-1-1 ESInet truly embodies a network-agnostic philosophy, a critical design choice made possible by our advanced SD-WAN (Software-Defined Wide Area Network) solution. Our ESInet is not bound to any single connectivity technology or provider; instead, it intelligently adapts across a multitude of network types. Our SD-WAN solution significantly enhances our underlying IP routing implementation by dynamically leveraging diverse connectivity options, including high-reliability MPLS circuits, cost-effective broadband connections, Low Earth Orbit (LEO) satellite links, and robust cellular capabilities. By using multiple providers for each of these diverse links, we build a foundation of unparalleled resilience and flexibility, ensuring that the ESInet services remain accessible and performant under all conditions.

SD-WAN: Closing the outage gap

Central to this network-agnostic approach is the SD-WAN overlay's ability to intelligently discover network paths in real time across the network. Operating with underlying routing protocols, the SD-WAN continuously monitors the performance metrics (such as latency, jitter, and packet loss) of every available MPLS, broadband, LEO, and cellular link from all active providers. This dynamic intelligence allows it to proactively select and steer critical 9-1-1 traffic over the optimal path at any given moment, ensuring the highest Quality of Service (QoS) and reliability. In the event of an outage or degradation on one link, the SD-WAN automatically and seamlessly reroutes traffic to a healthy alternative, guaranteeing an uninterrupted flow of emergency communications and robust connectivity for every PSAP, regardless of its location or available access technologies.

NGCS location-based routing

The essence of NG9-1-1 is saving lives by routing 9-1-1 calls to the right PSAP the first time. While other vendors continue to include legacy routing equipment as a part of their service to lower cost and speed up implementation without ever truly reaching an i3 state, Motorola provides our customers with location-based routing as part of the initial project plan, avoiding potential second cutovers for PSAPs or change orders to achieve i3 compliance. We have accomplished this by using NENA i3 end-state architecture, with the caller's location as the basis for determining which PSAP the call will be routed to, significantly reducing call transfer times.



Why does it matter?

Choosing a truly NG9-1-1 compliant solution is critical for the safety of Nebraska's citizens. Many organizations nationwide initially were not fully transitioned to NG9-1-1 by the chosen service provider, retaining legacy Selective Routers (LSRs) in their call flows. This failure to remove legacy equipment led to numerous outages that were disruptive to 9-1-1 emergency services.

As a result, we are now seeing mandates such as yours that are requiring the complete removal of the LSR from the 9-1-1 call flow. In addition, as long as these legacy components are in the call flow, the PSAPs will be unable to take advantage of location-based routing or new approaches to calls for service such as video and multimedia which require an IP network for delivery.

It will be critical for the Commission to ensure that the responses received truly comply with your requirement as stated. Implementing location-based routing from Day 1 is standard practice for Motorola.



Agnostic legacy and i3 interoperability

It is important that your i3 call routing platform can work seamlessly with both legacy and i3 routing systems that border Nebraska. The Motorola Call Routing Service exceeds this need in all our deployments across the country, and will support this interoperability for the Commission.

Multiple levels of redundancy – no single point of failure

The Motorola Call Routing Service is deployed in a highly resilient configuration. Multiple cloud providers, redundant network connections, and proactive monitoring all contribute to 99.999% operational availability. Our approach is to:

- Build a solution with leading software technology.
- Thoroughly test it, including end-to-end use cases, in our lab and as a part of the acceptance test.
- Deploy it in a geo-diverse, redundant configuration on public-safety grade infrastructure.
- Include services to closely monitor, secure, and manage the deployed solution.





Transparency through real-time status portal

Breaking through carrier obfuscation

The Motorola Call Routing Service includes a Customer Web Portal that gives PSAPs the visibility they need to ensure the integrity of their NGCS and Emergency Services IP Network. This will allow PSAPs to overcome the traditional carrier roadblocks to easily understand network health, configure policies, and more (depending on their roles), for 9-1-1 operational continuity and ongoing situational awareness.

Protecting the integrity of your 9-1-1 network and the safety of your community

The Commission and any of Nebraska's PSAP technical staff will benefit from real-time visibility into the technical health of your NGCS and ESInet network. Maps, graphs, and tables provide status details on call routing paths, applications, and IP network infrastructure. Tabs for alerts and notifications enable fast access to areas of concern. From this view, designated personnel can also manage events and understand maintenance events.

Manage open cases

The Commission's 9-1-1 stakeholders will have visibility of open cases related to network issues, as well as tools to create cases and stay aware of scheduled maintenance. Using this view of the Customer Web Portal, regional 9-1-1 directors, PSAP managers, Telecommunicators, and technical staff understand the status of their cases, including escalations, as well as trending issues. Service reports are available for download.

Access reports and analytics

Network and 9-1-1 administrators at state, regional, or even local levels will have easy access to reports upon demand. The Customer Web Portal makes this possible, providing NENA i3 event logging and network metrics, as well as enabling historical analysis. Interactive reports facilitate application and element drilldown for system transparency.

Why other customers are choosing our NGCS service

“Throughout the transition, three things were key: communication, education, and feedback. It also was critical that our vendor was already a trusted partner. The company explained things along the way and took the time to make sure we understood what was changing as we transitioned.”

– Anita Pitt, 9-1-1 manager for
Brazos Valley (TX) Council of Governments (BVCOG)



The right plan

Implementation, installation, migration

We will bring all of our experience and expertise in NG9-1-1 deployment and system support and management to ensure that your NG9-1-1 solution is implemented smoothly and performs at optimal capacity. From our initial meeting to the successful deployment of a solution aligned to your needs, with targeted training to ensure your personnel can work with ease on the new system, we will work as your partners to ensure a timely and efficient transition to a NG9-1-1 system.

Motorola's approach to implementation is characterized by our exceptional communication and transparency. Throughout the project, project personnel will have access to a live workbook that provides comprehensive, real-time updates on every aspect of the project. With one click, you can view the status of OSP migrations, PSAP i3 call readiness, location services, PSAP transfer requirements, action register, and more. This empowers identified personnel with unparalleled project oversight, ensuring alignment on current status and next steps, while also enabling you to provide real-time information to key stakeholders.

Project management and staffing

Motorola project managers know how to get the job done right. In fact, nearly many of our PMs have a background working in PSAPs and bring a deep understanding of critical environmental nuances during periods of change. A Motorola Solutions NG9-1-1 Program Manager will oversee a team of project management and engineering leaders, who will work closely with your project staff to ensure success. The project team will establish a project schedule that tracks tasks, milestones, start-end dates, and other factors, working directly with the Commission and Nebraska's identified PSAP personnel to optimize every aspect of implementation, training, product road mapping, and ongoing support to meet your needs.

Service and support

One of the most critical components to a successful NG9-1-1 deployment is the service and support you receive. Working with one partner who is not just the service provider but also the equipment manufacturer reduces risk and guarantees a smooth post-implementation experience.

Motorola will provide **one number to call** for any incidents related to NG9-1-1. Our dedicated 24/7 Network Security Operations Center (NSOC) will serve as the first point of contact during any incident. The local Motorola support team may be dispatched by the NSOC to resolve any issues that need in person attention.

Guaranteed project outcome

Our goal is to move the 9-1-1 traffic completely off the legacy selective routers. We understand the challenges of facility transition and collaboration with OSPs. It takes planning, expertise, and time. Anything short of a complete OSP migration can create additional costs for the Commission for routing (double billing), which can drag on excessively. We have observed many cases where non-Motorola customers were expected to absorb this cost uncertainty. This is not our approach. We will develop a comprehensive plan that will result in certainty of costs for the Commission.

Project risks and mitigation strategies

Having deployed multiple statewide and regional Next Generation Core Services across the country, we understand the potential implementation risks associated with these complex deployments. Our experience allows us to preempt and expertly navigate challenges such as the intricate setup of ingress and egress components, coordination with OSPs, and ensuring reliable PSAP connectivity. This puts Motorola in a unique position to make sure that those PSAPs understand the requirements and are prepared to ingest the new i3 data.



Investing in the future

From request for service to response, Motorola provides the entire ecosystem

Delivering the community's request for service to 911

Connecting the PSAP with field first responders



This is a pivotal moment for the Commission, and Motorola is uniquely positioned to support your transition to a next-generation public safety ecosystem. Selecting a call handling solution that integrates natively with your routing infrastructure ensures a seamless, end-to-end mission critical ecosystem that reduces technical complexity and maximizes system reliability.

Motorola provides a premier Next-Generation 9-1-1 (NG9-1-1) call handling ecosystem designed to streamline dispatch workflows and improve emergency response accuracy. Engineered for both state-wide, complex urban hubs and growing municipal environments, our solution transforms the emergency call experience by simplifying decision-making for telecommunicators. By reducing cognitive load, the platform allows call takers to remain focused on the caller while ensuring first responders receive vital, real-time information.

Our unified call handling approach is a highly customizable, NENA i3-standard software suite that provides an end-to-end mission-critical communications experience. Built for operational efficiency, it offers precise caller location, transcription assistance, and automatic abandoned callbacks. Our call handling system is designed to scale with evolving technological standards, and we will work side-by-side with your team to understand your specific operational requirements, ensuring the final system is customized to your unique workflows, staffing needs, and long-term vision for emergency services.

Our strategic approach optimizes technology to ensure a seamless flow of information from the initial call to case closure. With dedicated technical resources already on the ground in the region, Motorola is ready to be your local partner in establishing a new standard for public safety services in Nebraska.

A system for now and the future



The Motorola Solutions Next Generation 9-1-1 VESTA NXT Call Handling and Routing Service deployment not only met our expectations, but it also exceeded them. We now have a resilient, modernized emergency communications system that positions us well for the future. We are extremely pleased with the outcome and the professionalism shown throughout the project."

– William Q. Ramey, Director of Information Systems
Office of Public Safety / City of Chicago





Thank you

Thank you for the opportunity to present this proposal for the Commission's transition to NG9-1-1 call routing. We would be honored to continue our partnership and implement a solution that will deliver exceptional 9-1-1 service, which is vital for connecting individuals in need with help. Our team is 100% focused on helping you achieve the goals of this RFP, and we welcome further discussion regarding our proposal.

To learn more, visit: www.motorolasolutions.com



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2026 Motorola Solutions, Inc. All rights reserved. 04-2026 [BP04]

Table of Contents

Section 1

Corporate Overview.....	1-1
a. BIDDER IDENTIFICATION AND INFORMATION	1-1
b. FINANCIAL STATEMENTS.....	1-2
c. CHANGE OF OWNERSHIP	1-3
d. OFFICE LOCATION.....	1-3
e. RELATIONSHIPS WITH THE STATE	1-3
f. BIDDER’S EMPLOYEE RELATIONS TO STATE	1-4
g. CONTRACT PERFORMANCE	1-4
h. SUMMARY OF BIDDER’S CORPORATE EXPERIENCE	1-5
i. SUMMARY OF BIDDER’S PROPOSED PERSONNEL/MANAGEMENT APPROACH.....	1-9
j. SUBCONTRACTORS.....	1-24

Section 2

Response to Scope Of Work	2-1
Services to be Provided	2-1
1. ESInet Architecture and Design	2-1
2. NG911 Core Services (NGCS).....	2-2
3. GIS and Location-Based Routing	2-3
4. Call Flow and Media Session Handling	2-4
5. Security, Privacy, and Trust	2-4
6. Logging, Reporting, and Call Detail Records	2-5
7. Interoperability, Testing, Conformance, and System Acceptance.....	2-6
8. Operational Support and Service Level Agreements (SLAs).....	2-6
Applicable Standards	2-6
Federal Communications Commission Rules	2-8
Other Industry Standards	2-8
Conformance to Standards	2-9
Baseline Conformance.....	2-9
Gap Identification (Proposal Requirement)	2-9
Standards Updates (Post-Award).....	2-10
Non-Disclosure and Breach	2-10
Deviation Classification (Proposal Requirement)	2-10
Remediation Plan and Progress.....	2-11
Interoperability	2-11
NENA NG911 i3 Standard Conformance.....	2-12

Section 3

Response to Work Plan and Project Planning	3-1
1. Project Management	3-1
Governance and Leadership	3-1
Control of Scope, Schedule, and Budget	3-1
Risk and Issue Management	3-2
Stakeholder Communications and Status Reporting.....	3-2
Minimum PMP contents:	3-3
2. Staffing and Qualifications	3-3
3. Implementation	3-4
4. Transition	3-6
Minimum topics:	3-6
5. Testing and Acceptance	3-8
System Testing must address, at minimum:	3-9
Testing Methodology	3-10
Regression Testing and Defect Remediation.....	3-10
Documentation Methodology and Status Codes	3-11
Deficit Correction and Regression Testing	3-11

Section 4

Deliverables and Deliverable Approval Process.....	4-1
1. ESInet Architecture and Design :	4-1
System Requirements	4-1
Deliverables:	4-1
2. NG911 Core Services (NGCS)	4-2
System Requirements:	4-2
3. GIS and Location-Based Routing	4-2
System Requirements:	4-2
4. Security, Privacy, and Trust.....	4-3
System Requirements:	4-3
Deliverables:.....	4-3
5. Logging, Reporting, and Call Detail Records	4-3
System Requirements:	4-3
Deliverables:.....	4-3
6. Interoperability, Testing, Conformance, and System Acceptance	4-4
System Requirements:	4-4
Deliverables:.....	4-4
7. Operational Support and Service Level Agreements (SLAs)	4-4
System Requirements:	4-4
Deliverables:.....	4-4
Submission Requirements	4-5

Section 5

Technical Requirements 5-1

1. ESInet Requirements 5-1

1.1 Architecture and Topology 5-8

1.1.1 ESInet Diagrams..... 5-8

1.1.2 ESInet Interconnection 5-12

1.2 External and PSAP Connectivity..... 5-16

1.2.1 Originating Service Provider (OSP) Connection 5-16

1.2.2 PSAP Connection..... 5-19

1.3 Legacy Interoperability..... 5-21

1.3.1 Legacy Network Gateway (LNG)..... 5-21

1.3.2 Legacy Selective Router Gateway (LSRG)..... 5-27

1.3.3 Legacy PSAP Gateway (LPG)..... 5-30

1.4 Network Behavior and Performance 5-35

1.4.1 ESInet IP Routing 5-35

1.4.2 ESInet Bandwidth 5-38

1.4.3 Quality of Service (QoS) 5-40

1.4.4 Traffic Flow Requirements..... 5-42

1.4.5 Traffic Shaping 5-44

1.4.6 ESInet Network Time..... 5-45

1.5 Resilience and Service Levels..... 5-47

1.5.1 ESInet Availability..... 5-47

1.5.2 ESInet Reliability 5-49

1.6 Operations and Management..... 5-51

1.6.1 ESInet Monitoring and Management 5-51

1.6.2 ESInet Maintenance Window..... 5-54

1.7 Implementation Details..... 5-56

1.7.1 Port Mapping..... 5-57

2. Next Generation Core Services (NGCS) Requirements 5-58

2.1 Edge Security and Ingress..... 5-64

2.1.1 Border Control Function (BCF) 5-64

2.1.2 STIR/SHAKEN Support..... 5-69

2.1.3 Security Mechanisms 5-71

2.2 Core Routing and Location..... 5-76

2.2.1 Emergency Services Routing Proxy (ESRP) 5-76

2.2.1.1 Policy Store..... 5-81

2.2.2 Location Information Server (LIS)..... 5-83

2.2.3 Location Database (LDB) 5-88

2.2.4 Emergency Call Routing Function / Location Validation Function (ECRF/LVF) 5-93

2.2.5 Forest Guide 5-98

2.2.6 Service/Agency Locator (SAL)..... 5-100

2.3 Data and Enrichment..... 5-101

2.3.1 Additional Data Repository (ADR) 5-101

2.4 Call Flow and Media Handling..... 5-104

2.4.1 Call Flow and Session Handling Requirements 5-104

2.4.2 Media Quality of Service (QoS)..... 5-105

 2.4.2.1 Audio..... 5-105

 2.4.2.2 Video..... 5-107

 2.4.2.3 Text 5-108

2.4.3 Interactive Multimedia Response Service (IMRS) 5-111

2.4.4 Bridge 5-111

2.5 Egress and External Interfaces 5-115

2.5.1 Outgoing Call Interface Function (OCIF) 5-115

3. GIS and Database Services Requirements 5-116

3.1 Data Management and Interfaces 5-118

3.1.1 GIS and Database Management Functionality 5-118

3.1.2 Spatial Interface (SI) Functionality 5-123

3.2 Core Data Services 5-127

3.2.1 Mapping Data Service 5-128

3.2.2 MSAG Conversion Service (MCS)..... 5-129

3.2.3 Geocode Conversion Service (GCS) 5-131

3.3 PSAP-Facing Services..... 5-132

3.3.1 PSAP Mapping Service 5-132

3.3.2 Map Discrepancy Reporting..... 5-134

3.4 External Integrations 5-134

4. Security Requirements..... 5-135

4.1 Management and Process Control 5-136

4.1.1 Personnel Roles and Responsibilities..... 5-136

4.1.2 Identity Management..... 5-140

 4.1.2.1 Roles 5-146

4.1.3 Policies and Procedures..... 5-151

 4.1.3.1 Incident Response Plans 5-155

4.1.4 Authorization and Data Rights Management..... 5-162

4.2 Information System Infrastructure and Management 5-165

4.2.1 Device Inventory..... 5-165

4.2.2 Patching and Update Management 5-168

4.2.3 Segmentation and Traffic Separation 5-171

4.2.4 Network Boundary Protection..... 5-174

 4.2.4.1 External Connections..... 5-175

 4.2.4.2 Demilitarized Zones (DMZ)..... 5-178

 4.2.4.3 Defense in Depth 5-181

 4.2.4.4 Remote Access 5-185

4.2.5 Infrastructure Resilience 5-188

4.3 Authentication and Federated SSO..... 5-194

4.4 Cryptography and Public Key Infrastructure 5-198

4.4.1 Cryptographic Keys..... 5-203

4.4.2 Use of Self-Signed Certificates 5-209

4.5 Integrity Protection 5-212

4.5.1 JSON Web Signatures (JWS) 5-215

4.6 Information Privacy 5-218

4.7 Security Assessment and Audit 5-220

4.7.1 Assessment and Audit Documentation 5-222

4.8 Security Monitoring, Detection, and Alerting 5-225

4.8.1 Security Event Logging and Continuous Monitoring 5-225

 4.8.1.1 Time Synchronization 5-229

4.8.2 Denial of Service and Telephony Denial of Service (DoS/TDoS) 5-233

4.8.3 Intrusion Detection and Prevention Systems (IDS/IPS) 5-237

4.9 Domain Name System (DNS) 5-239

5. Reporting Services Requirements 5-244

5.1 Reporting and Data Collection Requirements 5-245

5.2 Logging Service 5-245

5.3 i3 Logging and Reporting Requirements 5-246

5.4 Functional Element Reporting 5-246

5.5 Monitoring, Outages, Failover, Trouble Tickets, and Escalation 5-248

5.6 Maintenance and Configuration Reports 5-252

5.7 Discrepancy Reporting 5-252

5.7.1 Policy and Core Routing 5-257

 5.7.1.1 Policy Store Discrepancy Report 5-257

 5.7.1.2 Policy Discrepancy Report 5-258

 5.7.1.3 Emergency Services Routing Proxy (ESRP) Discrepancy Report 5-258

5.7.2 Location and GIS Sources 5-259

 5.7.2.1 Location Information Server (LIS) Discrepancy Report 5-259

 5.7.2.2 GIS Discrepancy Report 5-259

 5.7.2.3 MSAG Conversion Service Discrepancy Report 5-260

 5.7.2.4 LoST Discrepancy Report 5-261

5.7.3 Signaling and Edge 5-264

 5.7.3.1 SIP Discrepancy Report 5-264

 5.7.3.2 Border Control Function (BCF) Discrepancy Report 5-265

5.7.4 Network and Infrastructure 5-267

 5.7.4.1 Network Discrepancy Report 5-267

5.7.5 Security and Trust 5-268

 5.7.5.1 Permissions/Security/Authentication Discrepancy Report 5-268

 5.7.5.2 Log Signature/Certificate Discrepancy Report 5-270

5.7.6 Data and Logging 5-271

 5.7.6.1 Logging Service Discrepancy Report 5-271

 5.7.6.2 ADR/IS-ADR Discrepancy Report 5-272

5.7.7 PSAP Operations and Treatments 5-273

 5.7.7.1 PSAP Call Taker Discrepancy Report 5-273

 5.7.7.2 Call Transfer Failure Discrepancy Report 5-274

5.7.7.3 Interactive Media Response (IMR) Discrepancy Report 5-275

5.7.8 External Providers 5-275

5.7.8.1 Originating Service Provider Discrepancy Report..... 5-275

5.7.9 Test and Tools 5-278

5.7.9.1 Test Call Generator Discrepancy Report..... 5-278

6. Installation Requirements 5-280

6.1 Installation Services 5-282

6.2 Wiring and Cabling 5-284

6.3 Grounding 5-286

7. Training 5-287

7.1 Audiences and Scope..... 5-288

7.2 Training Elements..... 5-289

7.3 Technical Assistance..... 5-290

7.4 Schedule and Locations..... 5-290

7.5 Training Materials 5-290

7.6 Post-Deployment Training and Costs (Proposal Requirement)..... 5-291

7.7 Comprehension, Testing, and Certification..... 5-291

7.8 Training Plan and Samples (Proposal Requirement) 5-292

8. Operations and Service Management Requirements..... 5-292

8.1 Service Management Framework 5-294

8.1.1 Service Management Plan..... 5-294

8.1.2 Service Level Agreement (SLA)..... 5-300

8.1.3 Compliance and Risk Management 5-301

8.1.4 Monthly Project Review and Compliance 5-308

8.2 Continuity and Resilience 5-309

8.2.1 Availability..... 5-309

8.2.2 Continuity of Operations Plan (COOP)..... 5-310

8.2.3 Disaster Recovery (DR)..... 5-312

8.3 Operations Centers and Support..... 5-314

8.3.1 Network Operations Center (NOC) 5-314

8.3.2 Security Operations Center (SOC) 5-320

8.3.3 Help Desk 5-324

8.3.3.1 Trouble Handling and Ticketing Requirements..... 5-326

8.3.3.2 Monitoring of Applications and Equipment..... 5-328

8.3.3.3 Root Cause Analysis..... 5-329

8.3.4 Customer Support Services..... 5-331

8.4 Monitoring and Event Management 5-338

8.4.1 Alarm Categories..... 5-338

8.5 Change, Maintenance, and Release Management 5-339

8.5.1 Change Management Requirements..... 5-340

8.5.1.1 Security Considerations in Change Management 5-343

8.5.2 Scheduled Maintenance Process 5-344

8.5.3 Software Development Process	5-348
8.5.4 Software Updates and Improvements.....	5-349
8.6 Spares and Inventory	5-353
8.6.1 Spares	5-353
8.6.2 Spare Inventory at Data Centers.....	5-357
9. Value Add and Optional Services	5-358
9.1 Call Handling Equipment (CHE) Services.....	5-359
9.2 ESInet and NGCS backup system.....	5-363
10. Use Case Examples for Use with Response	5-364
10.1 Instructions.....	5-364
10.2 Additional Examples	5-379
Section 6	
Cost Sheet.....	6-1
Section 7	
Response to Terms	7-1
Section 8	
Contractual Agreement Form	8-1
Section 9	
Technical Matrix	9-1
Section 10	
Exhibits.....	10-1
Exhibit 1 VESTA NXT Router NNI – Basic SIP OSP and Peer Interface Specification.....	10-2
Exhibit 2 VESTA NXT Router NNI Specification – i3 SIP OSP and Neighbor i3 Router	10-3
Exhibit 3 Prohibited Communications Equipment Affidavit.....	10-4
Exhibit 4 Sample Project Management Plan.....	10-5
Exhibit 5 Sample Project Schedule.....	10-6
Exhibit 6 Architecture and Topology Diagrams	10-7
Exhibit 7 NIOC PCA Validation Policy	10-8
Exhibit 8 NIOC PSAP Credentialing Agency PCA Certificate Policy	10-9
Exhibit 9 Service Level Agreement.....	10-10
Exhibit 10 Sample Support Plan.....	10-11

Section 1

Corporate Overview

The Corporate Overview section of the solicitation response should consist of the following subdivisions:

a. BIDDER IDENTIFICATION AND INFORMATION

The bidder should provide the full company or corporate name, address of the company's headquarters, entity organization (corporation, partnership, proprietorship), state in which the bidder is incorporated or otherwise organized to do business, year in which the bidder first organized to do business and whether the name and form of organization has changed since first organized.

Motorola Response

Comply.

Motorola has a strong presence with NG9-1-1 across North America, and a solid, experienced management, implementation, and ongoing support team already in place, ready to further serve the State of Nebraska.

Our headquarters is located at 500 W Monroe St. Ste. 4400 Chicago, IL 60661-3781. We are organized to do business in all 50 states, and have teams local to Nebraska.

Motorola has been an innovator in communication technology since our founding as the Galvin Manufacturing Corporation in 1928. From pioneering mobile communications in the 1930s, making equipment that carried the first words from the moon in 1969, to supporting modern-day emergency response equipment for disaster relief efforts worldwide, Motorola has a global footprint with products demonstrating our thought leadership. Motorola has roughly 21,000 employees globally that support our customers daily.

Motorola is uniquely positioned in our industry, as our sole focus is Public Safety. We are the only company that provides a complete suite of integrated Public Safety solutions and technologies, including:

- Next Generation Core Services.
- 9-1-1 Emergency Call Handling Solutions.
- Computer Aided Dispatch & Records Management Systems.
- Radio Dispatch, In Car, and Body Worn Cameras.
- Project 25 Radio Systems.
- Digital Evidence Management Systems.
- Video and Analytics, Incident Management.
- Real Time Intelligence.
- Jail Management.

b. FINANCIAL STATEMENTS

The bidder should provide financial statements applicable to the firm. If publicly held, the bidder should provide a copy of the corporation's most recent audited financial reports and statements, and the name, address, and telephone number of the fiscally responsible representative of the bidder's financial or banking organization.

Motorola Response

Motorola demonstrates a strong and stable financial position. This assessment is supported by consistent revenue growth, robust cash flow generation, and a record-breaking order backlog, all of which indicate sustained demand for the company's mission-critical technologies. Evidence of these findings can be obtained through our financial disclosures found at the following link:

[Investor Relations Homepage - Motorola Solutions](#)

As these reports are lengthy and have been provided via the link above. Physical copies are available upon request.

If the bidder is not a publicly held corporation, either the reports and statements required of a publicly held corporation, or a description of the organization, including size, longevity, client base, areas of specialization and expertise, and any other pertinent information, should be submitted in such a manner that solicitation evaluators may reasonably formulate a determination about the stability and financial strength of the organization. Additionally, a non-publicly held firm should provide a banking reference.

Motorola Response

Motorola is a publicly held corporation.

The bidder must disclose any and all judgments, pending or expected litigation, or other real or potential financial reversals, which might materially affect the viability or stability of the organization, or state that no such condition is known to exist.

Motorola Response

No such condition is known to exist. Motorola Solutions Connectivity, Inc. ("Motorola") is a wholly-owned subsidiary of Motorola Solutions, Inc., a Fortune 500 company with billions of dollars in annual sales globally, employing thousands of workers worldwide and having more than one hundred thousand (100,000) shareholders. As is normal for such companies, Motorola and its affiliates have been a party to many civil lawsuits. These suits have made many different legal and factual claims and have put forward many alleged legal theories seeking damages or other legal relief against Motorola affiliates. None of these matters are considered by Motorola or its parent to be material, and nor would they impact the ability of Motorola to perform this contract. As a publicly traded company, however, Motorola's parent files an annual report Form 10-K with the SEC and describes therein certain litigation

that is material for disclosure under SEC rules. Please see SEC filings. See Item 3, Legal Proceedings, [Motorola Solutions - 2025 10-K](#)

c. CHANGE OF OWNERSHIP

If any change in ownership or control of the company is anticipated during the twelve (12) months following the solicitation response due date, the bidder should describe the circumstances of such change and indicate when the change will likely occur. Any change of ownership to an awarded bidder(s) will require notification to the Commission.

Motorola Response

Understood.

d. OFFICE LOCATION

The bidder's office location responsible for performance pursuant to an award of a contract with the State of Nebraska should be identified.

Motorola Response

Comply.

Office location is:

500 W Monroe St. Ste. 4400

Chicago, IL 60661-3781

e. RELATIONSHIPS WITH THE STATE

The bidder should describe any dealings with the State over the previous ten (10) years. If the organization, its predecessor, or any Party named in the bidder's solicitation response has contracted with the State, the bidder should identify the contract number(s) and/or any other information available to identify such contract(s). If no such contracts exist, so declare.

Motorola Response

For the past decade, the partnership between the State of Nebraska and Motorola Solutions has been on the implementation and maintenance of a statewide public safety communications network. A central element of this collaboration is the Statewide Radio System (SRS), a P25 digital platform

providing interoperable communication for first responders, 911 dispatch centers, and public utilities across all 93 counties.

While we previously operated under Contract 14534 OC, we transitioned in 2024 to a new agreement, Contract 111563 O4. This current contract has a five-year term with the option for two additional five-year renewals. These agreements ensure the continued supply and maintenance of public safety communication products and services. Our partnership remains dedicated to protecting the State's investment through consistent system upgrades and long-term support.

f. BIDDER'S EMPLOYEE RELATIONS TO STATE

If any Party named in the bidder's solicitation response is or was an employee of the State of Nebraska within the past six (6) months, identify the individual(s) by name, State agency with whom employed, job title or position held with the State, and separation date. If no such relationship exists or has existed, so declare.

Motorola Response

Comply.

No such relationships exist.

If any employee of any agency of the State is employed by the bidder or is a subcontractor to the bidder, as of the due date for solicitation response submission, identify all such persons by name, position held with the bidder, and position held with the State (including job title and agency). Describe the responsibilities of such persons within the proposing organization. If, after review of this information by the State, it is determined that a conflict of interest exists or may exist, the bidder may be disqualified from further consideration in this solicitation. If no such relationship exists, so declare.

Motorola Response

Comply.

No such relationships exist.

g.CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past ten (10) years, all such instances must be described as required below. Termination for default is defined as a notice to stop performance delivery due to the bidder's non-performance or poor performance, and the issue was either not litigated due to inaction on the part of the bidder or litigated and such litigation determined the bidder to be in default.

Motorola Response

Motorola has no contracts that were terminated for default.

It is mandatory that the bidder submit full details of all termination for default experienced during the past ten (10) years, including the other Party's name, address, and telephone number. The response to this section must present the bidder's position on the matter. The State will evaluate the facts and will score the bidder's solicitation response accordingly. If no such termination for default has been experienced by the bidder in the past ten (10) years, so declare.

Motorola Response

As discussed above, Motorola has had no agreements terminated for default.

If at any time during the past five (5) years, the bidder has had a contract terminated for convenience, non-performance, non-allocation of funds, or any other reason, describe fully all circumstances surrounding such termination, including the name and address of the other contracting Party.

Motorola Response

As a result of a new statewide implementation in the State of Pennsylvania, Motorola customers Chester County, Pennsylvania, Greene County, Pennsylvania and Lackawanna County, Pennsylvania terminated their agreements with Motorola's predecessor entity, Vesta Solutions, Inc, in February of 2023. The sole reason for such termination was those entities transitioning to the statewide system in Pennsylvania.

h.SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

The bidder should provide a summary matrix listing the bidder's previous projects similar to this Solicitation in size, scope, and complexity. The State will use no more than three (3) narrative project descriptions submitted by the bidder during its evaluation of the solicitation response.

The bidder should address the following:

- Provide narrative descriptions to highlight the similarities between the bidder's experience and this Solicitation. These descriptions should include:
- The time period of the project, The scheduled and actual completion dates,
- The bidder's responsibilities,
- For reference purposes, a customer name (including the name of a contact person, a current telephone number, a facsimile number, and e-mail address); and

- Each project description should identify whether the work was performed as the prime vendor or as a subcontractor. If a bidder performed as the prime vendor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.

Motorola Response

Comply. Three references are provided below.

State of Utah Communications Authority (UCA) - Statewide NG9-1-1 Call Routing and Call Handling

Melanie Crittenden – 911 Division Director

Phone: (801) 840.4223

Mcrittenden@uca911.org

Motorola is pleased to share details regarding our successful partnership with the State of Utah Communications Authority (UCA).



- With a population of nearly 3.3 million, (UCA awarded Motorola the contract as the prime vendor following a statewide competitive procurement process, to migrate its 43 PSAPs to a NENA i3-compliant NGCS, ESInet, and a statewide VESTA 9-1-1 call handling as a service platform.
- The deployed solution is delivering a 99.999% highly available and redundant solution that exceeds UCA's requirements which are similar to the requirements set forth in this RFP solicitation, specifically sections 1-5 & 9. The proposed solution enhanced 9-1-1 services through location-based routing and it eliminated the reliance UCA had on the Telco's (Lumen Technologies) legacy selective routers in the State of Utah by completing OSP migrations.
- The UCA contract was executed in June 2020 with an initial budget of \$29,974,132 and a negotiated completion date of February 2022. The project stayed on track from a timeline and budget perspective. UCA has executed an additional 5 year contract extension through June 2030. In September of 2022 a Federal site (Hill Air Force Base) in Utah took advantage of the UCA contract and was added to the Motorola NENA i3-compliant NGCS and ESInet platform. This addition was completed on time in March of 2024, meeting all Federal and JITC requirements.

Greater Harris County, Texas - Regional NG9-1-1 Call Routing

Roger Hauck - Services Director

832-237-9911

Sheffern@911.org



Motorola is pleased to share details regarding our successful partnership with Greater Harris County (GHC), Texas.

- With a population of roughly 5.8 million, GHC awarded Motorola the contract as the prime vendor to migrate its 45 PSAPs to a NENA i3-compliant NGCS and ESInet platform in November of 2017.
- GHC's plan to procure a market-ready solution capable of agnostic interoperability between call-routing and the existing VESTA Hosted call-handling solution, and to all current and future external NG9-1-1 solutions operational in neighboring agencies became a reality as the dedicated Motorola implementation team met all contractual milestones, delivering a 99.999% highly available and redundant solution that exceeded GHC's expectations and solicitation requirements which are similar to the requirements set forth in this RFP solicitation, specifically sections 1-5. The proposed solution enhanced 9-1-1 services through location-based routing and it eliminated the reliance GHC had on the Telco's (AT&T & Lumen) legacy selective routers in the region by completing OSP migrations.
- The GHC contract was executed in November 2017 with an initial budget of \$14.3 million and a negotiated completion date of January 2019. The initial project was completed on time in January 2019 within the approved \$14.3 million budget. Following this success, GHC renewed the NGCS/ESInet contract for an additional five-year term in December 2022. During this renewal, Motorola performed additional work to meet evolving requirements. We achieved full project completion in July 2024, remaining within the total contract budget of \$20,681,490.60.

State of New Mexico - Statewide NG9-1-1 Call Routing

Stephen A. Weinkauff - NM911 Bureau Chief

Phone: 505-660-3637

Stephen.Weinkauff@dfa.nm.gov



Motorola is pleased to share details regarding our successful partnership with the State of New Mexico.

- With a population of just over 2.1 million, the State of New Mexico is the 36th largest in the nation. Following a statewide competitive procurement process, the New Mexico Department of Finance and Administration (NMDFA) awarded Motorola the contract as the prime vendor to migrate its 42 primary and 11 secondary PSAPs to a NENA i3-compliant NGCS and ESInet platform, including Text-to-911 capabilities.
- Motorola's dedicated implementation team met all contractual milestones, delivering a 99.999% highly available and redundant solution that exceeded NMDFA's requirements which are similar to the requirements set forth in this RFP solicitation, specifically sections 1-5. The proposed solution enhanced 9-1-1 services through location-based routing and it eliminated the reliance NMDFA had on the Telco's (Lumen Technologies) legacy selective routers in the State of New Mexico by completing OSP migrations.
- The NMDFA contract was executed in July 2023 with an initial budget of \$14,010,149.32 and a negotiated completion date of January 2025. By successfully integrating customer-requested design enhancements and helping the customer navigate PSAP readiness requirements, we reached full project completion in July 2025. These strategic adjustments perfectly tailored the final solution to the environment's evolving needs, resulting in a total investment of \$15,022,964.19.

-
- I. Bidder and Subcontractor(s) experience should be listed separately. Narrative descriptions submitted for Subcontractors should be specifically identified as subcontractor projects.

Motorola Response

Understood

- II. If the work was performed as a subcontractor, the narrative description should identify the same information as requested for the bidders above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

Motorola Response

Understood

i. SUMMARY OF BIDDER'S PROPOSED PERSONNEL/MANAGEMENT APPROACH

The bidder should present a detailed description of its proposed approach to the management of the project.

The bidder should identify the specific professionals who will work on the Commission's project if their company is awarded the contract resulting from this solicitation. The names and titles of the team proposed for assignment to the Commission project should be identified in full, with a description of the team leadership, interface, and support functions, and reporting relationships. The primary work assigned to each person should also be identified.

Motorola Response

Comply.

Motorola's project management methodology is built on a foundation of partnership, reliability, accountability, and transparency. Our approach provides a structured framework for successfully implementing NG9-1-1 services, drawing on extensive experience in deploying complex public safety solutions.

The project begins with a Project Kick-off Meeting to introduce team members, review roles, and establish the initial project schedule and communications plan. Following this, we enter a Detailed Design Review (DDR) phase to gather information specific to the State's operational environment, validate technical requirements, and finalize the baseline project schedule.

Throughout the implementation, Motorola will use a combined Project Management Plan (PMP) and Project Schedule to provide a consistent vehicle for communication, progress reporting, and the proactive detection of potential delays.

Proposed Project Team

Motorola has assembled a cohesive team of specialists to work as a collaborative partner with the State of Nebraska. These individuals are top-tier experts in their respective fields, selected specifically for their experience in delivering high-priority public safety solutions.

The following chart outlines our team structure, including our Executive Escalation contact to ensure rapid decision-making and project accountability.

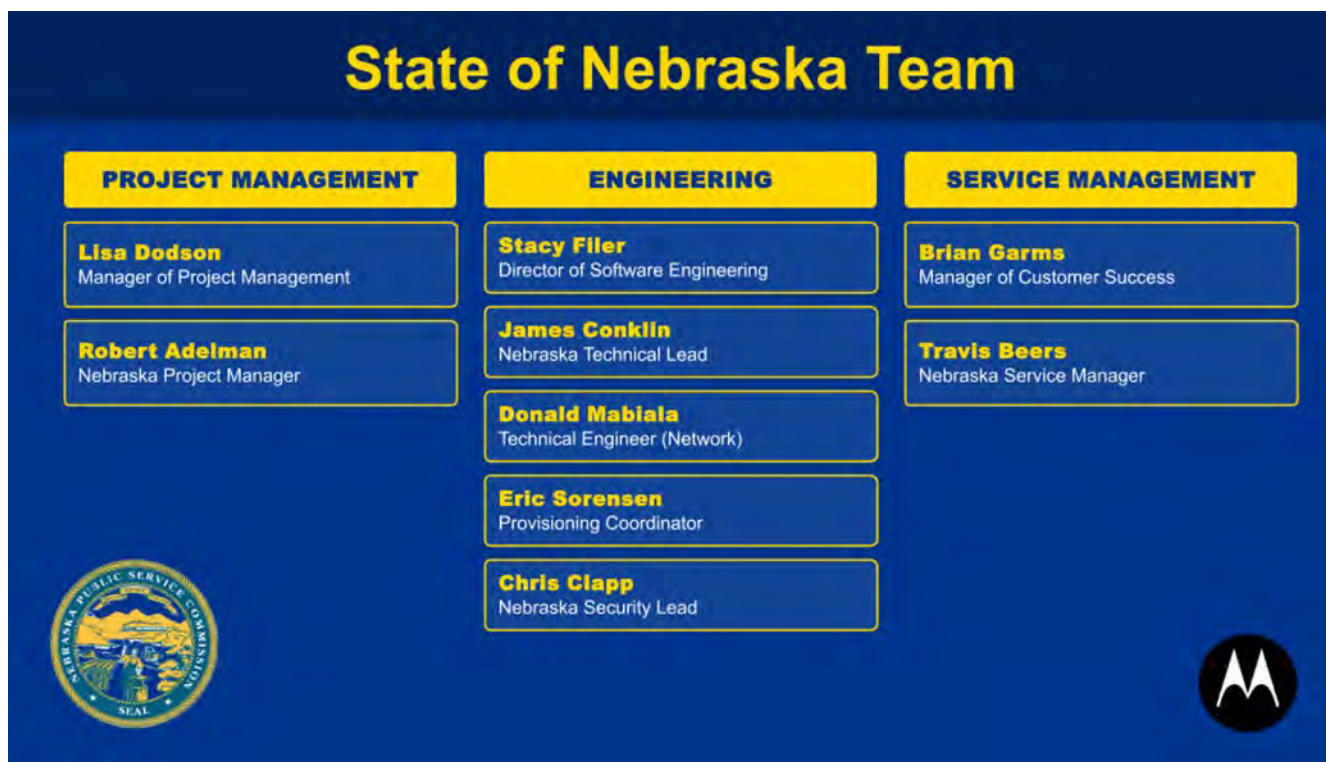


Figure 1-1: Motorola Nebraska Team

Team Leadership and Support Functions

The project will be led by a dedicated **Project Manager** who serves as the primary point of contact and sole authority for project actions and reporting. This individual is responsible for enforcing performance standards, controlling risks, and managing the project's cost and quality.

The core leadership team is further supported by the following specialized roles:

- **Project Manager** : Primary POC; lead decision-making authority for project duration.
- **Lead NGCS Engineer / Solutions Architect**: Responsible for the overall system design, ensuring the technical integrity of the core routing service and ESInet WAN connectivity.
- **Network Solution Architect / Technical Engineer**: Designs and implements the network infrastructure for VESTA NXT Router.
- **Network Implementation Manager / Provisioning Coordinator**: Supplements the Project Manager and Lead Engineer by serving as the single point of contact for carriers and coordinating the rollout of ESInet circuits.
- **CSM**: Manages the contracted maintenance and support services, serving as a post-implementation point of contact to ensure SLAs are maintained.
- **Cyber Security Lead/Manager**: Manages security posture, including patching, backups, and audits.

Reporting Relationships and Primary Work Assignments

Table 1-1: Reporting Relationship and Work Assignments

Full Name & Title	Primary Work Assigned	Reporting Relationship
Robert Adelman Project Manager	Overall project management, contract terms, schedule, risk management, and quality assurance.	Lead authority; reports to project stakeholders.
James Conklin, Lead NGCS Engineer (Technical Lead)	System design, equipment configuration, hardware/software integration, and technical integrity of the NGCS design.	Reports to the Project Manager.
Donald Mabiala, Network Solution Architect (Technical Engineer)	Design and implement the network infrastructure for VESTA NXT Router.	Reports to the Project Manager.
Eric Sorensen, Network Implementation Manager (Provisioning Coordinator)	Circuit path orders, tracking Firm Order Completion (FOC) dates, and coordinating with carriers for circuit turn-up.	Supports the Project Manager and Lead Engineer.
Travis Beers, Customer Service Manager (Service Manager)	Maintenance and support management, creating the support plan, and overseeing change management during operations.	Liaison between the State and Motorola's support organization.
Chris Clapp, Security Lead	Manages security posture, including patching, backups, and audits.	Manages security posture, including patching, backups, and audits.

Motorola maintains a cross-trained resource pool to ensure that project continuity is preserved throughout the life of the implementation. If a need for staffing changes arises, we will work with the State to designate new resources with the requisite skills and experience.

The bidder should provide resumes for all personnel proposed by the bidder to work on the project. The Commission will consider the resumes as a key indicator of the bidder's understanding of the skill mixes required to carry out the requirements of the solicitation in addition to assessing the experience of specific individuals.

Resumes should not be longer than three (3) pages. Resumes should include, at a minimum, academic background and degrees, professional certifications, understanding of the process, and

at least three (3) references (name, address, and telephone number) who can attest to the competence and skill level of the individual.

Motorola Response

Comply.

Motorola provides the following resumes for the primary personnel assigned to the State of Nebraska project. These individuals have been selected based on their extensive experience in public safety and their proven ability to execute NG9-1-1 implementations.

Each resume highlights the individual's academic background, professional certifications, and a deep understanding of the implementation process specific to their role. Motorola acknowledges the State's requirement for references and has included at least three contacts for each professional who can attest to their competence and skill level.

These professionals represent a team of seasoned experts. Except in the most unavoidable circumstances, Motorola will maintain member continuity throughout the project life cycle.

Robert Adelman, Project Manager

Robert M. Adelman, ENP, PMP - NGCS Sr. Project Manager

Phone: (210) 870-7616 / (210) 300-7101

Email: robert.adelman@motorolasolutions.com

Qualifications and Experience

Robert has 30+ years in public safety. For the past 6 years, as NGCS Sr. Project Manager with Motorola, Robert currently manages the delivery of our Next Generation Core Services (NGCS) products and services to 9-1-1 authorities transitioning to Next-Generation 9-1-1 (NG9-1-1). As a member of our NGCS Delivery team, Robert leads our team members in all aspects of assigned projects, responsible for delivering contract scope, on schedule and within budget, while maintaining customer satisfaction. Prior to joining Motorola, Robert spent 25 years in the public sector managing public safety communications and 9-1-1 operations for a large urban county in south-central Texas. Robert is a Master Peace Officer and currently serves as the Special Projects & Technology Officer, Local Agency Security Officer, and Terminal Agency Coordinator for the Olmos Park Police Department. Robert chairs the Alamo Area Council of Governments (AACOG) Interoperable Communications Committee and chairs the FCC Region 53 700 & 800 MHz Regional Planning Committees.

Key Projects/Achievements with Motorola Solutions

- Brazos Valley COG, TX (NGCS)
- Central Texas COG, TX (NGCS)
- Heart of Texas COG, TX (NGCS)
- Golden Crescent RPC, TX (NGCS)
- Sarasota County, FL (both NGCS and Call Handling)
- Collier County, FL (NGCS)
- Martin County, FL (NGCS)
- Manatee County, FL (NGCS)
- St. Lucie County, FL (both NGCS and Call Handling)
- Galveston County ECD, TX (NGCS)
- McLennan County EAD, TX (NGCS)
- Ector County ECD, TX (NGCS)
- Midland County ECD, TX (NGCS)
- State of New Mexico (NGCS) – Implementation Underway (47 PSAPs / 45 CHS)

Relevant Work History

- Motorola (2019 – Present)
- Olmos Park Police Department, TX
- Bexar County Sheriff's Office, TX

Education, Certifications, and Memberships

- Bachelor's Degree in Criminal Justice, St. Mary's University, San Antonio, TX
- PMI Project Management Professional (PMP)
- NENA Emergency Number Professional (ENP)
- Master Texas Peace Officer
- Level 4 CJIS Security
- IS-100, IS-200.a, ICS-300, G-400, IS-700.a, IS-701.a, IS-703.a, IS-704, IS-800.b
- Chairperson, AACOG Interoperable Communications Committee
- Chairperson, FCC Region 53, 700 & 800 MHz Regional Planning Committees
- AACOG Delegate, Texas SCIP Executive Council (SEC)

References

Name: Stephen Weinkauf, NM911 Bureau Chief (New Mexico Department of Finance & Admin)

Address: 407 Galisteo St, Santa Fe, NM 87501

Telephone Number: (505) 660-3637

Email: Stephen.Weinkauf@dfa.nm.gov

Name: Brett Schneider, Chief Executive Officer (Bexar Metro 9-1-1 Network)

Address: 911 Saddletree Court, Shavano Park, TX 78231

Telephone Number: (210) 316-4020

Email: bschneider@bexarmetro.org

Name: Stacy Filer, Engineering Director – NGCS Managed Services (Motorola Solutions)

Address: 500 West Monroe Avenue Chicago IL 60661

Telephone Number: (847) 417-4908

Email: stacy.filer@motorolasolutions.com

James Conklin, NGCS Solution Architect

James Conklin - Senior Solutions Architect/Manager

Phone: 951.365.1765

Email: james.conklin@motorolasolutions.com

Qualifications and Experience

James Conklin has been employed by Motorola since 2014. He is an experienced manager and team leader providing NGCS engineering direction for the design, deployment, and integration organizations. For Motorola, James has operated in several architecture, security, and engineering roles and currently works as a Senior Manager of Systems Engineering. His team is responsible for solution architecture and engineering of the NGCS product offerings, working with the implementation, engineering, design, security, and sales teams to establish and maintain products and services that meet and exceed market requirements. With more than 25 years of experience in system design, test, and delivery, he brings a wealth of experience to the Motorola team.

Key Projects/Achievements

James' experience provides the project management team's leadership a valuable resource throughout all phases of the project. His support in the design, delivery, management, and implementation of complex and high-priority initiatives range from Motorola developed software to custom-designed initiatives to meet customer needs. His recent projects include:

- Federal and Department of Defense (DoD) sites (over 130 world-wide locations).
- Florida (Escambia, Collier, Manatee, Martin, Lee, St. Lucie and other counties).
- Nevada (Las Vegas Metro Police Department [LVMPD] and North Las Vegas Police Department [NLVPD])
- New Mexico, state-wide contract
- Utah, state-wide contract
- Texas (Lubbock Emergency Communication District [LECD], and multiple Councils of Government [COGs]).

Relevant Work History

- Motorola
- Before joining Motorola, he worked for numerous large and small companies including Ocean Systems Engineering Corporation (OSEC), Vencore, QinetiQ North America (QNA), and Cassidian Communications/Airbus DS Communications. Prior to that, he was enlisted in the United States Marine Corps.

Education, Certifications, and Memberships

- MS in Cyber Security Operations and Leadership from University of San Diego.
- BA in Intelligence Analysis from American Military University.
- Certified Information Systems Security Professional (CISSP), (ISC)2, 2016—Present.

References

Name: Stacy Filer

Address: Chicago, IL

Telephone Number: 847.417.4908

Name: Eric Sorensen

Address: Denver, CO

Telephone Number: 720.724.4982

Name: Sam Bard

Address: Austin, TX

Telephone Number: 847.417.4908

Travis Beers, Customer Service Manager

Travis Beers - Lead Customer Service Manager

Phone: (330) 802-4273

Email: Travis.Beers@motorolasolutions.com

Qualifications and Experience

A dedicated and results-driven Customer Success professional with 15+ years of experience in public safety and telecommunications. Proven ability to translate complex technical solutions into critical customer value, ensuring operational excellence, and driving high-stakes challenge resolution. Committed to transforming deep technical data into actionable insights that improve product adoption, streamline processes, and build long-term, unbreakable client partnerships. Career progression includes roles as an Escalation Manager for Call Handling Support and subsequent promotion to Lead Customer Service Manager (CSM) for the entire Central Region.

Key Projects/Achievements

- Indianapolis, IN: Led a large-scale Premier One CAD hardware refresh and integration across all of Indiana and its hosted sites, encompassing over 2,000 standard CAD clients and mobile units.
- Lake County, IN: Managed the comprehensive integration and upgrade project for Command Central Aware.
- Porter County, IN: Successfully implemented the first ASAP to PSAP Premier One CAD integration with an upgraded data interface, collaborating with Mission Critical Partners.
- St Charles County, MO: Directed the Callworks Hardware refresh spanning eight Public Safety Answering Points (PSAPs) with two data centers. This is an NGCS site with dual redundancy closed loop MPLS data circuits.
- As the Escalation Manager for the Emergency Call Handling Support help desk, I managed high priority incidents for all of Motorola's Next-Generation Core Services (NGCS) customers. My responsibilities included developing comprehensive Root Cause Analyses and presenting them to the customers.

Relevant Work History

- Motorola Solutions
- Intrado: Supported VIPER call handling systems, building foundational expertise in public safety telecommunications.

Education, Certifications, and Memberships

- Cleveland State University Alumni
- Certifications: CJIS certified
- Core Competencies:
- 15+ years in public safety, emergency management and telecommunications.
- Expertise in translating deep technical complexities into clear, actionable data and business insights.
- VESTA, Premier One CAD, Flex CAD, Command Central Aware, Callworks.

References

Name: Commander Brad Bosse (Lake County, IN)

Address: 2293 N Main St, Crown Point, IN 46307, USA

Telephone Number: (219) 755-3400

Name: Craig Beringhaus (Cincinnati, OH)

Address: 2000 Radcliff Dr, Cincinnati, OH 45204

Telephone Number: (513) 242-6616

Name: Director of 9-1-1 Deborah Wiley (Huber Heights, OH)

Address: 6121 Taylorsville Road, Huber Heights, OH 45424

Telephone Number: (937) 233-1565

Eric Sorensen, Network Implementation Manager

Eric Sorensen - Provisioning Coordinator

Phone: (720) 724-4982

Email: eric.sorensen@motorolasolutions.com

Qualifications and Experience

Telecommunications professional with over 30 years of experience, primarily in public safety communications. Involved with 9-1-1 from Basic services to today's NG9-1-1 technologies. Supported the development of new standards for 9-1-1 in many venues. Key accomplishments:

- Managed implementation operations, project management, customer training, and technical training for Intrado Viper E9-1-1 CPE systems.
- Coordinated integration of Viper systems deployments with ESInet and Txt29-1-1 services.
- Created CLEC entity (Intrado Communications) to support deployment of 9-1-1 voice services (A911).
- Initiated and maintained all regulatory filings required for Intrado Communications CLEC.
- Developed international market opportunities for emergency communications services from Intrado.
- Key manager for a Chinese joint venture company selling location-based emergency call processing in China.
- Member Board of Directors for a Chinese joint venture company.
- Managed deployment of outsourced E9-1-1 database management services for the State of Texas and all associated COGs.
- Member TR45.2 standards committee for creation of Wireless E9-1-1 network standards
- Architected one of the earliest demonstrations of wireless location information delivery with 9-1-1 calls.
- Managed design and roll out of initial Wireless 9-1-1 services from Intrado.
- Demonstrated Automatic Crash Notification delivery to 9-1-1 PSAPs in 1999.
- NENA Board Member.
- Co-Creator of NENA Technical Development Conference (TDC); later became NDC and NENA Standards and Best Practices conference.
- 9-1-1 Product Director for Pacific Bell through California statewide E9-1-1 deployment.

Key Projects/Achievements

At Motorola Solutions, Inc.

- Works closely with the Sales and Engineering teams to deliver customer-driven, world-class, leading-edge, end-to-end network solutions that rise to the challenges of first-responder 9-1-1 customers across the country.
- Facilitates timely order issuance and service delivery with multiple service partners.
- Coordinates resolution of service issues and concerns to complete systems deployment per customer expectations and engineering designs.
- **Prior to Motorola Solutions, Inc.**
- Led Implementation Operations team delivering project management, field installation, and customer/technical training support for all Intrado Viper CPE deployments across the U.S. and Canada.
- Coordinated infrastructure deployment and product launch for business IP voice services throughout New Zealand. Assured quality service introduction coordinated across internal and external organizations. Ensured quality end-to-end customer experience.
- Defined and implemented a new strategic subsidiary for implementation of telecom network services. Managed all regulatory certification and compliance for the new subsidiary. Supervised Carrier Relations team and interconnection contract negotiation.
- Drove international market development efforts. Defined target markets, market entry strategy, and appropriate offerings to establish and grow Intrados' international market presence in alignment with corporate strategies. Helped establish XieAn Intrado Int'l, a joint venture company in China. Country experience includes EU, China, SE Asia, India, and New Zealand/Australia.
- Directed the team delivering a multi-million dollar service contract supporting implementation and billing of E9-1-1 database services for the State of Texas. Managed all aspects of data operations, program management, customer support, budget, forecasting, staffing, and organizational strategic planning.

Relevant Work History

- Motorola Solutions, Inc.
- West Safety Services.
- Spark/Telecom New Zealand.
- Reliance Globalcom.
- Intrado Inc.
- Pacific Bell.

Education, Certifications, and Memberships

- Bachelor of Science – Business Administration; Pepperdine University.
- CJIS Level 4 Security Training.
- Lean Six Sigma Certification-Villanova University.
- Advanced Management Training Certificate-Duke University (Fuqua School of Business).

References
Name: Bryant Underwood Address: Paradise, TX Telephone Number: 940-252-0102
Name: Cindy Alderete Address: Houston, TX Telephone Number: 713-410-5911
Name: David Walker Address: Camdenton, MO Telephone Number: 513-314-6763

Donald Mabiala, Network Solution Architect

Donald Mabiala, Network Solution Architect Phone: (725) 251-0039 Email: donald.mabiala@motorolasolutions.com
Overview As a Network Solutions Architect (NSA) on the NGCS Prime team, I design and implement the mission-critical network infrastructure for Next Generation IP Selective Routing, supporting state-wide 9-1-1 call delivery across North America. My role ensures high system availability and responsive service delivery through robust architecture, infrastructure management, strategic planning, and operational excellence.
Experience / Key Projects - Architect and Implement Next Generation Core Services and Emergency Services IP Network - Design and Deploy Statewide, County, and Jurisdiction Projects from 2021-26 - Built multiple geographically redundant NGCS hosted and on-premise data centers - Design and Deploy F5 LTM WAF subsystems for New York City PSAC1 & 2. - Integrated advanced security including SSL, offloading and geolocation enforcement - New York City NGCS Networking & Lab Build - Successful planning and execution of move, add, change projects across North America.
Companies

- Motorola Solutions
- Credit One Bank
- Ericsson

Education and Certifications

- Associate's Degree in Computer Science
- Google Project Management Certification
- Cisco Certified Network Professional Routing & Switching
- Cisco Certified Network Professional Security
- Juniper Networks Certified Associate
- F5 LTM & ASM/WAF Certification
- Arista VeloCloud SD-WAN Certification

References

Name: Chris Clapp

Address: Temecula, CA

Telephone Number: 951.440.7850

Name: Wes Nakama

Address: Chicago, IL

Telephone Number: 310.989.6047

Name: Stacy Filer

Address: Chicago, IL

Telephone Number: 847.417.4908

Chris Clapp, Cyber Security Lead

Chris Clapp, Cyber Security Engineer III

Phone: (951) 551-4208

Email: chris.clapp@motorolasolutions.com

Qualifications and Experience

- A valued member of Motorola since 2006, Chris has held several sequentially more critical positions culminating in his current position as a Senior Cyber Security Engineer. During this progression, Chris has designed and supervised the deployment of security and response solutions covering over 1200 PSAPs in the United States, including networking devices, host-based solutions, and centrally and locally managed patching/vulnerability controls solutions along with centralized anti-virus deployments.
- In his current position, Chris is responsible for the design and deployment of security controls for the Next Generation call routing solutions. In this position, he develops industry-leading technical and operational defense technologies and techniques to defend 9-1-1 systems from internal and external threats and actors.
- Chris has over 20 years of experience in Systems Administration, Networking, Security, and Telephony Solutions.

Key Projects / Experience

- State of Florida VESTA Router design and implementation of security infrastructure covering service to a ~5m user-base.
- Originated a secure and highly available compartmentalized design for second and third generation 9-1-1 call routing functions covering 25m users.
- Greater Harris County (Houston): Design and deployment of security solutions for call handling, call routing, and GIS services.
- New York City: Design and deployment of security solutions for the United States largest single Call Handling Solution.

Relevant Work History

- Motorola
- Before joining the team at Motorola, Chris worked for ViaSat Communications.

Education, Certifications, and Memberships

- Masters of Science, Cybersecurity
- BS Cybersecurity and Information Assurance
- Certified Information Systems Security Professional (CISSP).
- Cisco Certified Network Professional (CCNP).

- Microsoft Certified Systems Engineer (MCSE).

References

Name: Jen York

Address: 26400 Beachwood Road, Menifee, CA 92584

Telephone Number: 951-551-3208

Name: Dave Park

Address: PO Box 1128, Seligman, AZ, 86337

Telephone Number: 951-551-1225

Name: Nick Finly

Address: 32662 Safflower St, Winchester, CA, 92596

Telephone Number: 951-249-1803

Any changes in proposed personnel shall only be implemented after written approval from the Commission.

Motorola Response

Comply

j. SUBCONTRACTORS

If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide:

- I. name, address, and telephone number of the subcontractor(s),
- II. specific tasks for each subcontractor(s),
- III. percentage of performance hours intended for each subcontract; and
- IV. total percentage of subcontractor(s) performance hours;
- V. whether the subcontractor is affiliated with the bidder or has common ownership.

Please note the definition of “subcontractor” in the glossary in providing a proper response to this.

Motorola Response

No subcontractors or consultants are anticipated for the execution of this project.

Section 2

Response to Scope Of Work

Bidder should read the Scope of Work Section of this RFP and provide a response as part of its proposal. This response should describe how the bidder will complete the scope of work, fill in any additional steps or details necessary, and demonstrate why the bidder is the most qualified or capable.

Additional Note: The response should not contain any reference to dollar amounts. However, information such as data concerning labor hours and categories, materials, subcontracts and so forth, may be considered so that the bidder's understanding of the scope of work may be evaluated.

Motorola Response

Understood

Services to be Provided

The scope of this RFP encompasses the full lifecycle of the NG911 system, from design and implementation to operations and decommissioning. A comprehensive listing of the minimum technical requirements needed to operationalize a proposed solution is located in §E (Technical Requirements) of this document.

1. ESInet Architecture and Design

- a. Contractor shall provide an ESInet design and implementation conforming to the NENA i3 ESInet architecture and functional requirements, including multi-site, geographically diverse redundant cores, session border control at boundaries, and tenant isolation. (This includes bandwidth provisioning, diagrams, availability, and reliability features).

Motorola Response

Comply.

- b. Contractor shall support IPv4 and IPv6 addressing, implement Quality of Service (QoS) (DiffServ or equivalent) to prioritize emergency signaling and media, and document bandwidth and capacity needs for all services. (This includes referenced 99.999 requirements that will be included in the Service Level Agreement (SLA)).

Motorola Response

Comply.

- c. Contractor shall support SIP signaling per RFC 3261 and required NG911 SIP extensions (SIP over TLS for signaling, and SRTP for media, where used), and demonstrate SIP interconnects with external peers. (This includes SIP call flow across the ESInet, no calls “lost,” and conversion where necessary).

Motorola Response

Comply.

- d. Contractor shall provide documented peering and interconnect interfaces (LNG, LSRG, LPG, SBCs and other edge elements, Points of Interconnection) and APIs and procedures for peering with other ESInets and third-party providers. (Configuration management database, diagrams, IP schema).

Motorola Response

Comply.

We have provided our published NNI Documentation as attachments, Exhibit 1 VESTA NXT Router Service NNI Specification Basic SIP OSPs and Peer NGCS Interface and Exhibit 2 VESTA NXT Router Service NNI Specification i3 SIP OSPs Neighbor i3 Router

2. NG911 Core Services (NGCS)

- a. Contractor shall provide or interoperate with NGCS functional elements (FEs) (BCF, ESRP, ECRF, LVF/LIS, MSAG/ALI-equivalent services, ESRP/ESRP-like routing proxy, etc.) as defined in the NENA i3 Standard and shall map which product components implement each NGCS function.

Motorola Response

Comply.

- b. Contractor shall implement NGCS interfaces per the NGCS Interface Standard (SIP and REST interfaces, expected message formats including PIDF-LO where applicable) and shall provide interface documentation, schemas, and test harness endpoints.

Motorola Response

Comply.

Interface documentation, Schemas, and test harness endpoints are provided as part of the final As-Built documentation, which will be included as part of the Project Manager's concluding project documentation.

- c. Contractor shall meet stated latency and throughput SLAs for NGCS lookups and routing decisions. (99.999 from caller to call-taker unless specified in writing between the PSC and Contractor.)

Motorola Response

Comply.

3. GIS and Location-Based Routing

- a. Contractor shall accept, store, and use GIS data in the NENA GIS data model/schema and SHALL maintain the required NENA layers (PSAP boundaries, ESN/service boundaries, address points, civic addressing, emergency routing attributes). GIS data shall conform to normative language identified in NENA-STA-006.2-2022. The Contractor may utilize NENA-REF-006.2-2023 (NENA NG9-1-1 GIS Data Model Templates) to assist in conformance to the Standard.

Motorola Response

Comply.

- b. Contractor shall use authoritative GIS data for routing decisions (ECRF) and shall accept location in PIDF-LO format (and convert civic/geodetic input) for routing and display.

Motorola Response

Comply.

- c. Contractor shall provide GIS data versioning, change tracking, import/export in NENA formats (e.g., GML/GeoJSON or NENA schema), and support automated incremental updates.

Motorola Response

Comply

4. Call Flow and Media Session Handling

- a. Contractor shall implement NENA i3 call flows (incoming SIP INVITE → ESRP/ECRF lookup → PSAP routing) preserving required SIP headers (P-Asserted Identity, Diversion, History Info, etc.) and shall deliver PIDF-LO location payloads with calls where required.

Motorola Response

Comply.

- b. Contractor shall support real-time multimedia as defined by NENA (voice, IP text-to-911, real-time video, and supplemental data) with media negotiation, fallback behaviors, and preservation of metadata across transfers.

Motorola Response

Comply.

- c. Contractor shall support PSAP call transfer (warm or attended and blind transfers) while preserving call metadata and location.

Motorola Response

Comply.

5. Security, Privacy, and Trust

- a. Contractor shall implement the NENA ESInet security and trust model including mutual TLS between NG911 elements, strong authentication and RBAC for administrative interfaces, and secure boundary elements (SBCs).

Motorola Response

Comply.

- b. Contractor shall encrypt sensitive data in transit (TLS 1.2+ / TLS 1.3) and at rest (AES-256 or equivalent), provide PKI/certificate lifecycle management, and protect cryptographic keys using a hardware security module or equivalent. Contractor shall support certificate revocation.

Motorola Response

Comply.

-
- c. Contractor shall provide incident response and vulnerability management processes and supply recent third-party penetration test reports and remediation plans.

Motorola Response

Comply.

- d. Contractor shall satisfy Neb. Rev. Stat. 86-125 by completing the affidavit provided by the State regarding the use of prohibited communications equipment by communications providers.

Motorola Response

Comply.

Motorola acknowledges this requirement and will provide the completed affidavit as requested (Exhibit 3 Prohibited Communications Equipment Affidavit).

6. Logging, Reporting, and Call Detail Records

- a. Contractor shall produce end-to-end logs and Call Detail Records (CDRs) for every emergency transaction containing timestamps and share with the data analytics engine, correlation IDs, call identifiers, caller identity (if available), location used for routing, PSAP destination, media types, and call disposition.

Motorola Response

Comply.

- b. Contractor shall provide secure storage of logs and CDRs, role-based access controls, and export capability in open formats.

Motorola Response

Comply.

- c. Contractor shall provide operational reports (call volume, answer times, transfers, location failure rates, outage reports) and support ad-hoc queries.

Motorola Response

Comply.

7. Interoperability, Testing, Conformance, and System Acceptance

- a. Contractor shall participate in jurisdiction-specified interoperability and conformance testing, independent third-party validation and verification, demonstrate NGCS and ESInet interfaces in a test harness, and provide test results and logs.

Motorola Response

Comply.

- b. Contractor shall provide full product documentation, API specifications, training, runbooks, and operator and administrator manuals.

Motorola Response

Comply.

8. Operational Support and Service Level Agreements (SLAs)

- a. Contractor shall negotiate with the PSC to establish firm SLAs for availability, incident response, escalation, mean time to repair (MTTR), change management procedures, and maintenance windows.

Motorola Response

Comply.

- b. Contractor shall produce a rollback and contingency plan for major updates that affect routing/GIS or call handling.

Motorola Response

Comply.

Applicable Standards

Respondents must demonstrate their industry knowledge and describe their commitment to proposing standards-based NG911 solutions and services.

Motorola Response

Comply.

Motorola is deeply committed to advancing and deploying standards-based NG9-1-1 solutions. With nearly a century of experience in public safety communications, including over 55 years in 9-1-1 call handling and over 35 years in 9-1-1 call routing, our industry knowledge is extensive and foundational to our offerings.

Commitment to Industry Standards and Leadership Motorola actively participates in and holds leadership roles across key Standards Development Organizations (SDOs) such as NENA, APCO, and the Alliance for Telecommunications Industry Solutions (ATIS). Our personnel serve on and co-chair critical NENA working groups, including the i3 Architecture, NG-PSAP Systems, GIS Data Stewardship, and Security for NG9-1-1 committees.

To ensure ongoing interoperability and standards alignment, Motorola has participated in every NENA Industry Collaboration Event (ICE) to date. During these events, we rigorously test our products alongside other vendors to validate compliance across various aspects of the i3 architecture, including call routing, logging, multimedia, and security. We also maintain prominent roles in the Industry Council of Emergency Response Technology (iCERT) and the NG9-1-1 Interoperability Oversight Commission (NIOC).

NENA i3 Compliance Our proposed NGCS solution is fully compliant with NENA i3 standards, including the detailed functional and interface specifications outlined in NENA-STA-010. We enthusiastically embrace the NENA i3 end-state architecture by delivering true location-based routing for 9-1-1 calls on Day 1, ensuring calls are routed to the correct PSAP based on caller location rather than legacy cell-sector routing.

All core functional elements provided in our solution are designed to meet or exceed NENA i3 functional specifications, including:

- Emergency Services Routing Proxy (ESRP)
- Emergency Call Routing Function (ECRF)
- Location Validation Function (LVF)
- Policy Routing Function (PRF)
- Border Control Function (BCF)
- Spatial Interface (SI)
- Location Database (LDB)

By maintaining strict adherence to these open standards and protocols, Motorola ensures that our solutions provide seamless agnostic interoperability. This prevents proprietary lock-in, ensures reliable integration with existing and future systems, and allows agencies to connect securely with neighboring jurisdictions and diverse call-handling equipment.

The State may disqualify or reject non-standard or proprietary systems that may hinder NG911 implementation, limit interoperability, or that might restrict the State from interconnecting to a regional or national 911 system in the future.

Motorola Response

Understood.

Throughout the duration of this contract, Respondents SHALL maintain conformance with all standards listed in this Scope of Work and ensure that the products, solutions, and services provided for the State of Nebraska evolve and adapt as the standards evolve. A listing of currently approved NENA standards can be found at <https://www.nena.org/page/standards>.

Motorola Response

Comply.

In their response, Respondents must explain in detail how their proposed solution conforms to the requirements of the referenced standards.

Motorola Response

Understood.

Federal Communications Commission Rules

The Federal Communications Commission (FCC) regulates 911 services through various rules and requirements, primarily found in **47 CFR Part 9**, covering Enhanced 911 (E911), Text-to-911, Next Generation 911 (NG911), and location-based routing. Key requirements include transmitting all 911 calls, providing call-back numbers and precise location data, ensuring service for text and multimedia, and meeting standards for digital, IP-based systems and network reliability.

Motorola Response

Comply.

Other Industry Standards

All equipment proposed to support or operate within the State of Nebraska NG911 System must comply with relevant industry standards and reference models, including, but not limited to:

- American National Standards Institute (ANSI)
- Electronic Industries Alliance (EIA)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- Open Systems Interconnection (OSI)
- Telecommunications Industry Association (TIA)

- Underwriters Laboratories (UL)

Motorola Response

Comply.

Respondents must propose a system that utilizes an Open Standards Methodology:

- The proposed system shall be subject to standards that enhance open standards and increase interoperability such as ITU, IEEE 802 at OSI Layer 2, and IP and TCP, as defined by the IETF in the applicable RFCs, at OSI Layer 3 and above.

Motorola Response

Comply.

- If proprietary standards or protocols are used within a proposed solution, Respondents shall disclose the proprietary nature and discuss any limitations that may result.

Motorola Response

Comply.

Conformance to Standards

Baseline Conformance

The State prefers full conformance with **NENA-STA-010.3** at System Acceptance. The solution must remain current with NENA standards as they evolve. The State understands some limitations may require additional development.

Motorola Response

Comply.

Gap Identification (Proposal Requirement)

Respondents shall identify any gaps to full **NENA-STA-010.3** conformance in their proposals. Respondents are solely responsible for disclosing such gaps and providing a plan and timeline to close them.

Note:

The State recognizes that no existing implementation fully conforms to NENA-STA-010.3 (and many still have gaps against NENA-STA-010.2). Proposals must explicitly state all areas where the delivered system will not conform at time of delivery.

Motorola Response

Comply.

Standards Updates (Post-Award)

Contractors shall implement any new or changed feature required by an upgraded or revised NENA standard **within nine (9) months** of the standard's ratification for public use. The Contractor must supply regular progress reports for features and functions that are in revision. If at any point in the 9 month window the Contractor becomes aware that they will not meet the deadline they must inform the State in writing with an adjusted timeline for when the new features or functions will be delivered. If the Contractor cannot meet this timeline, it must request a **waiver**, including an alternative plan and schedule to achieve conformance.

Motorola Response

Comply.

Non-Disclosure and Breach

Exceptions to conformance must be explicit. Notwithstanding any other provision in the contractual terms, if the system is delivered with a **material deviation** from **NENA-STA-010.3** that was **not** disclosed in the proposal, and the State determines (in its sole discretion) the omission was **not** accidental, the Contractor will be deemed **in breach** of contract. If the State determines the omission was accidental, the State and Contractor will negotiate in good faith a deadline by which conformance must be achieved.

Motorola Response

Comply.

Deviation Classification (Proposal Requirement)

Each deviation must be classified as one of the following:

- **NENA-STA-010.3 upgrade, proposed date:** The delivered system conforms for the feature, and the proposal includes an estimated date for providing the **NENA-STA-010.3** upgrade to the State (no later than **Contract Year 2**).

- **Missing capability, proposed date:** The delivered system does **not** conform to NENA-STA-010.3 for the feature; the proposal includes an estimated upgrade date (no later than **Contract Year 2**).
- **Missing capability, no proposed date (will be provided):** The delivered system does not conform to **NENA-STA-**
- **010.2 or NENA-STA-010.3** for the feature; the proposal commits to provide the capability but does not specify a date.
- **Missing capability, no plans:** The delivered system does not conform and there is no intention to conform. An alternative to the **NENA-STA-010.3** feature may be proposed for State consideration.

Motorola Response

Comply.

Remediation Plan and Progress

Non-conforming features shall be listed in a **Remediation Plan** included with the proposal, identifying each feature and the estimated schedule. The Contractor shall update the Remediation Plan **at least quarterly**. The State expects reasonable, continuous progress. If any features remain non-conforming to **NENA-STA-010.3** by the end of **Contract Year 2**, the Contractor will be deemed **in breach** of contract.

Motorola Response

Comply.

Interoperability

The system must interoperate with any system conforming to **NENA-STA-010.3** that must interwork with the State's system. The State understands interoperability issues can arise from either party's non-conformance or from ambiguities in the standard. In such cases, the Contractor, the other vendor, and (as appropriate) the State's consultants shall work cooperatively to determine the non-conformance and corrective actions, using the **intent of NENA-STA-010.3** as the guiding objective.

- If the Contractor is required to make changes, it shall propose a completion date acceptable to the State.
- If the issue lies with the other vendor, the Contractor shall cooperate in testing but has no further responsibility.
- If the other vendor conforms to **NENA-STA-010.2**, the State's system conforms to **NENA-STA-010.3**, and the issue falls outside the **010.3** backward-compatibility statements for **010.2**, the Contractor is **not** required to make changes.

Motorola Response

Comply.

NENA NG911 i3 Standard Conformance

The following section includes references to conformance with **NENA-STA-010.3**. The absence of an explicit reference **DOES NOT** imply the State does not require conformance to that portion of the Standard. The State requires conformance to the full standard, while recognizing the practicalities of achieving conformance within the contract period as described above.

If the proposed system does not apply NENA Standards throughout the ESInet, the proposal must identify each deviation, explain why the Standard is not met, and propose an alternative.

Motorola Response

Comply.

Additional explicit Standards-conformance requirements appear in other sections of this RFP.
RESPONDENTS MUST COMPLETE THE STATUS TABLE BELOW.

Status must be presented with one of the following options:

- Implemented
 - The requirement is tested, approved, and in production.
- Roadmap – with timeframe in months
 - The requirement is not in production for any reason.
 - **Timeline** for implementation **MUST be within 12 months** of RFP Response.
- Future Planned
 - The requirement is not in production for any reason, and the planned implementation is ***longer than 12 months***.
- Not implemented
 - The requirement is not in production, and no plans have been developed for deployment/implementation of the requirement.

Table 1: NENA-STA-010.3 (i3 Standard) Conformance Status Matrix

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
ElementState and ServiceState	Allows a PSAP/State management app to see the status of each service (ESRP, ECRF (Emergency Call Routing Function)) and each "box" in a non-proprietary way	Roadmap - 4 months
All i3v3 interfaces plus i3v2 for backwards compatibility	REST/JSON interfaces conforming to i3v3 standard YAML with backwards compatibility to the i3v2 SOAP/XML interfaces	Roadmap - 10 months
Security Posture	Allows routing rules to take securitystate (green/yellow/orange/red) into account	Roadmap - 10 months
IPv6	Allows every element to have a public address and get calls/data from modern nets (wireless) without translation	Roadmap - 10 months
DNS based redundancy model	All services implement a redundancy model where more than one IP address is returned for the service URI, and any address can be used for a transaction	Roadmap - 4 months
History Info/Reason	Provides a logged reason why a call was not delivered the "normal" way	Implemented

Video	<i>Supports video calls to 911. Most importantly, allows deaf callers using VRS to be seen by call takers. Includes BCF, Bridge and logging service support</i>	<i>Future Planned</i>
MSRP	<i>Instant Messaging Service</i>	<i>Implemented</i>
Non-Human Initiated Calls	<i>Support for IoT devices, alarms, etc.</i>	<i>Implemented</i>
TLS (Transport Layer Security) transport of SIP	<i>Provides secure call signaling</i>	<i>Roadmap - 4 months</i>
SRTP	<i>Provides secure media (voice, video, text) for calls</i>	<i>Roadmap - 4 months</i>
RTCP support on all SIP entities	<i>Provides secure control of RTP (Real Time Transport Protocol) streams</i>	<i>Implemented</i>
RTCP Extended Reports	<i>Provides diagnostic information on media streams</i>	<i>Future Planned</i>

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
PSAP detection of loss of RTP vs silence	Differentiates silent calls from mechanical loss of audio media stream	Implemented
Element Overload (RFC 7339)	Graceful coping with too many SIP calls	Future Planned
STUN/TURN/ICE	Standards based mechanisms for NAT Traversal	Implemented
NG-AACN Support	Update to Automatic Car Crash Notification standards	Future Planned
SIP Presence for location	Allows OSPs to send location updates for mobile devices without manual rebid (requires OSP to implement also).	Future Planned
Policy Store i3v3 interface	Interoperable policy repository that allows 3rd party editors/verifiers/etc.	Implemented
Multiple Geolocation	Accepts more than one location reported in a 911 call	Implemented
Discrepancy Reporting mechanism + i3v3 defined DRs (Discrepancy Report)	Standardized way to report discrepancies with standardized responses	Implemented
Bad Actor mechanism	Allows PSAP to stop repeated bad calls from a source	Roadmap - 10 months
Call Suspicion mechanism	Allows the system to mark calls that MAY be bad, and then treat them specially at the PSAP (warnings, specialqueues, etc.)	Roadmap - 10 months

<i>QueueState</i>	<i>Allows Policy routing based on queue congestion</i>	<i>Implemented</i>
<i>DequeueRegistration</i>	<i>Allows multiple PSAPs and other entities to dequeue from a queue</i>	<i>Roadmap - 10 months</i>
<i>ESRPnotify</i>	<i>Allows policy routing rule to notify some entity that a condition was encountered</i>	<i>Roadmap - 10 months</i>
<i>AbandonedCall</i>	<i>Standardized way to report a call that was hung up before PSAP got the call</i>	<i>Roadmap - 7 months</i>

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Service/Agency Locator	Service that allows discovery of things on any ESInet rather than provisioning it.	Implemented
XACML based data rights management	Standardized way to control who has access to what data	Future Planned
EIDO on Transfer	Mechanism to transfer call state to a PSAP along with the call	Implemented
3rd Party Origination	Allows a 3rd party, like Video Relay Interpreter, to be automatically added to a call as a 3 way	Future Planned
RTT	Real Time Text support, includes multiparty RTT (Real Time Text) support (RFC 9071) and mixer support for non-aware devices	Implemented
Resource Priority header	Allows SIP Resource Priority handling of SIP messages. All SIP entities support it, BCF polices/inserts it.	Implemented
Incoming Baudot is converted to RTT	TTY to/from OSP converted to Real Time Text by LNG (Legacy Network Gateway) (Baudot to RFC 4103)	Future Planned
Outgoing Baudot is converted to RTT	TTY to/from PSAP converted to Real Time Text by LPG (Legacy PSAP Gateway) (Baudot to RFC 4103)	Future Planned
Multipart MIME (BCF, bridge, media server)	Allows multiple SIP bodies. Typically, this is Location by Value plus SDP.	Implemented

<i>SRV records for SIP interface resolution (BCF/ESRP and PSAP)</i>	<i>Standard mechanism to derive SIP connection address from a domain name</i>	<i>Implemented</i>
<i>Support for Outbound (RFC 5626)</i>	<i>SIP Protocol fixes for outbound calls</i>	<i>Future Planned</i>
<i>i3v3 Syntax and Semantics for Policy Routing Rules</i>	<i>Standardized Syntax and Semantics for Policy Routing Rules</i>	<i>Implemented</i>
<i>SBC inserts NENA-Source parameter</i>	<i>Allows PSAP to identify which SBC (BCF component) handled a call. Used with Bad Actor</i>	<i>Roadmap - 10 months</i>
<i>ESRP supports AdditionalData dereference for PRR</i>	<i>Allows policy routing based on additional data</i>	<i>Roadmap - 10 months</i>

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
<i>ESRP handles incoming admin calls</i>	<i>Allows policy routing of admin calls</i>	<i>Future Planned</i>
<i>ESRP policy routes calls to other agencies</i>	<i>Allows calls to other PSAPs, responders, to be policy routed. Includes extraction of location from an EIDO</i>	<i>Implemented</i>
<i>Support for incoming identity validation</i>	<i>STI-VS implemented to return STIR/SHAKEN validation on incoming calls.</i>	<i>Roadmap - 4 months</i>
<i>Gap/Overlap</i>	<i>Tells agencies about gap or overlap discovered by ECRF/LVF in GIS data</i>	<i>Implemented</i>
<i>ECRF handles any standard shape</i>	<i>Location can be specified by polygon, circle, ellipse, or arc band, in addition to point</i>	<i>Implemented</i>
<i>ECRF returns service boundary</i>	<i>ECRF can return a polygon, within which, the response will still be valid</i>	<i>Implemented</i>
<i>ECRF Supports lost-planned-changes</i>	<i>allows planned changes in GIS to occur on a schedule</i>	<i>Future Planned</i>
<i>matchType and degradedMatch implemented</i>	<i>Allows querier to know how validation was determined and receive a warning that validation was not necessarily as good as intended</i>	<i>Implemented</i>
<i>i3v3 Appendix B/NG GIS implemented</i>	<i>Updated GIS provisioning data model</i>	<i>Implemented</i>
<i>Support CLDXF location</i>	<i>US profile of PIDF-LO, FGDC conformant.</i>	<i>Implemented</i>

<i>Internal and External ECRF/LVF supplied</i>	<i>ECRF and LVF (Location Validation Function) for public and OSP support available on the Internet, separate from internal ECRF/LVF available on ESInet</i>	<i>Roadmap – 1 month</i>
<i>ECRF/LVF replica support</i>	<i>Interface that allows an OSP or other entity to maintain a local copy of the ECRF/LVF</i>	<i>Future Planned</i>
<i>Interconnected ESInet support</i>	<i>Allows neighboring ESInets to connect to the State ESInet. Supports bidirectional ECRF/LVF query, call transfer, etc.</i>	<i>Implemented</i>
<i>Forest Guide Support</i>	<i>Entry in FG for State ECRF/LVF, and recursive resolution of out of area queries via the FG</i>	<i>Roadmap – 9 months</i>

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
MCS (MSAG Conversion Service) and GCS (Geocode Conversion Service) are implemented	MCS = MSAG (Master Street Address Guide) Conversion Service, converts between MSAG form of address and PIDF-LO. GCS=Geocode conversion service, provides civic to geo, or geo to civic conversion for any system	MCS - Implemented GCS - Future Planned
Change in GIS results in routing change in minutes	A change in the GIS data can affect routing within minutes of the GIS authority releasing the change	Implemented
MDS implemented	Map Database Service returns maps (as images) or features to support both local and out of area maps	Future Planned
Spatial Interface is implemented	Standard was to provision ECRF/LVF/MDS/GCS/MCS	Implemented
Changes to PRR effective on next call	Update of PRR policy in Policy Store causes changes in routing immediately	Implemented
i3v3 DR interface and all defined DRs implemented	Automated Discrepancy Reporting mechanism and several standard DR formats	Implemented
i3v3 Test call is supported	Automated mechanism to test the call path. No human required. Includes media check (loopback)	Roadmap - 10 months
i3v3 Test Call Generator supported	Automated mechanism to generate test calls (can text PRR sets)	Roadmap - 10 months
IS-ADR search supported at PSAP	Standardized way to check outside sources to see if they	Roadmap - 10 months

	<i>have additional data for a telephone number</i>	
<i>humintlang tag supported</i>	<i>Signals request for language used on a call</i>	<i>Roadmap - 10 months</i>
<i>Call Transfer follows i3v3 call flows</i>	<i>Either Ad hoc or Route All Calls Via a Conference Aware UA (User Agent) model is followed for bridge based attended transfer</i>	<i>Implemented</i>
<i>Transfers between ESInets with different bridge models supported</i>	<i>Transfer of calls between ESInets that have different bridge models work as defined in the i3V3 standard</i>	<i>Implemented</i>
<i>Media server supports i3v2 IMR</i>	<i>Standardized multimedia "Interactive Voice Response" unit (auto answer with menus). Includes audio, video, text, RTT. Includes VXML for control.</i>	<i>Roadmap - 6 months</i>

v3 Standard Requirements	What Does It Do?	Status in Proposed Solution? (Implemented, Roadmap [with timeline in months], Future Planned, Not Implemented)
Logging service supports all i3v3 LogEvents	Logging Service supports all i3 defined log events	Implemented
NGCS elements create the specified LogEvents	All NGCS elements generate all V3 standardized log events they should implement	Implemented
Logger logs media per the standard	Logging service logs all media per the standard	Implemented
Logger retrieval interface follows standard	Logging Service implements i3 standardized log retrieval interface	Implemented
Logger can be used as IRR (Instant Recall Recorder)	Logging Service implements the Instant Recall Recorder function	Implemented
LNG supports P-Preferred-Identity + ESN/IMEI for non-initialized mobile	LNG retrieves IMEI for non-initialized phones and passes it in SIP P-Preferred Identify header	Future Planned
Outgoing Call Interface Function	Supports call backs and other outgoing calls with all media supported on the incoming emergency call. Includes support for STIR/SHAKEN signing of Identity.	Roadmap - 4 months

Section 3

Response to Work Plan and Project Planning

This section defines the required plans, methods, staffing, testing, and governance for implementing, accepting, and operating the NG911 solution. In this section and throughout this document (and as noted in the Glossary), **‘Respondent’** refers to the proposing entity pre-award, and **‘Contractor’** refers to the awarded entity post-negotiation and post-award. Any references to **‘Vendor’** identify any third party from whom the Respondent or Contractor (as applicable) procures goods or services to fulfill the requirements of this RFP and subsequent contract, including hardware, software, connectivity services, and external personnel.

1. Project Management

a. Project Management Approach

The Respondent shall describe a project management approach aligned with Project Management Institute (PMI) best practices and informed by the Information Technology Infrastructure Library (ITIL) for service transition and operations. The approach must cover governance, control of scope, schedule, and budget, risk and issue management, stakeholder communications, and status reporting. Post-award, the Contractor shall execute this approach.

Motorola Response

Comply.

Motorola’s project management methodology is built on a framework designed for the successful implementation of complex, integrated public safety solutions. The approach utilizes a combined Project Management Plan (PMP) and Project Schedule rooted in ITIL to ensure consistent communication, progress reporting, and the proactive detection of potential delays.

Governance and Leadership

- **Dedicated Leadership:** A designated Program Manager and Project Manager lead all project team members through the implementation process.
- **Single Point of Contact:** For post-implementation, Motorola provides a single point of contact to ensure continuity and a streamlined transition.
- **Collaborative Planning:** The preliminary PMP is further developed in direct partnership with the customer and submitted as a formal document during the DDR.

Control of Scope, Schedule, and Budget

- **Methodological Framework:** The project team follows a methodology that includes a Project Implementation Plan and a detailed Migration/Cutover Plan to deliver the project on time and within budget.

- **System Acceptance:** Governance includes a 30-day Reliability Test to ensure the system meets all contractual requirements before being deemed accepted and live.
- **Milestone Management:** Motorola utilizes a Project Dashboard to track progress against milestones, ensuring rigorous control over the project timeline.

Risk and Issue Management

- **Proactive Mitigation:** The Project Manager is responsible for identifying risks, communicating them to the team, and formulating plans to ensure a successful cutover with minimal disruption to PSAP operations.
- **Technical Oversight:** A Senior Technical Lead remains with the project until all PSAPs are transitioned to the Service to mitigate technical risks during migration.
- **Issue Resolution:** Punch lists are documented and resolved collaboratively with the customer to meet all criteria for final system acceptance.

Stakeholder Communications and Status Reporting

- **Consistent Communication:** The PMP serves as the primary vehicle for communicating the agreed-upon project plan, current status, and next steps to all stakeholders.
 - **Structured Meetings:** Final project closeout involves specific meetings to verify that all contract deliverables have been satisfied and to address any remaining questions.
 - **Documentation Delivery:** Motorola provides comprehensive "As-built" documentation, including policy route plans, escalation processes, and network path diversity drawings, prior to final acceptance.
-

b. Project Manager

The Respondent shall assign a dedicated **Project Manager (PM)** as the single point of contact. The PM is responsible for scope, schedule, budget, resources, risks, and stakeholder communications; must hold the Project Management Professional® (**PMP**) certification; and have **≥5 years'** experience leading projects of comparable size and complexity, preferably in public safety or telecommunications.

Motorola Response

Comply.

c. Preliminary Plan (Project Management Plan [PMP])

The Contractor shall develop and maintain a living PMP consistent with PMI. The PMP will be used to monitor and control installation and deployment and must be kept current with State visibility and approval of changes via the Change Management process.

Motorola Response

Comply. See our Exhibit 4 Sample Project Management Plan and Exhibit 5 Sample Project Schedule.

Minimum PMP contents:

- **Work Breakdown Structure (WBS), scope, deliverables, and schedule** (with milestones and the explicit handoff from implementation to service management).
- **Quality Assurance and Quality Control (QA/QC)** processes and acceptance criteria.
- **Risk and issue management** (registers, mitigation strategies).
- **Change Management Plan and Configuration Management Plan.**
- **Communications and Status Reporting Plan** (cadence, formats, dashboards, programmatic notifications).
- **Deployment and transition plan and schedule**, including a PSAP-by-PSAP work plan.

Notes:

- The PMP will be referenced regularly during implementation to ensure timely completion. -
- Any schedule or work-plan changes require prior State approval through the Change Management process. -

Motorola Response

Comply.

2. Staffing and Qualifications

a. Key Personnel

Identify **Key Personnel** (e.g., Project Manager, Technical Lead, Security Lead, Service Manager, Technical Engineer/Coordinator, Provisioning Coordinator). Provide resumes showing experience, qualifications, and relevant certifications. The State reserves approval rights for all Key Personnel and subsequent changes. Provide **30 days' written notice** before a Key Person's departure.

Motorola Response

Comply.

Motorola identified Key Personnel resumes are provided in the Staffing section of our response. Resumes highlighting their experience, certifications, and relevant public safety expertise are included in the Staffing section of this response.

b. Staff Qualifications

The contractor shall supply qualified, experienced personnel devoted to successful contract performance and, upon State request, remove or replace Key Personnel.

Motorola Response

Comply.

c. Designations, Certifications, and Licenses

Provide evidence that assigned personnel – especially Key Personnel – hold the professional designations, certifications, and licenses necessary to perform their roles effectively.

Motorola Response

Comply.

While employee credentials are confirmed in the provided resumes, Motorola maintains a policy of protecting the personal and sensitive information of our employees. Therefore, copies of physical certificates, licenses, or diplomas will be provided for verification to the State's satisfaction upon request during the contract negotiation phase. Motorola ensures all assigned staff will meet or exceed the qualification requirements throughout the project lifecycle.

3. Implementation

a. Implementation Approach

The Respondent shall describe an end-to-end approach for implementing ESInet and NGCS to deliver NG911 to all PSAPs. The State will assist with coordination and scheduling; the Contractor is responsible for planning and executing all activities. No service, system, or function is Accepted until the State provides written approval after successful testing and cutover readiness.

Motorola Response

Comply.

Motorola employs a comprehensive, end-to-end implementation approach designed to transition all Nebraska PSAPs to a robust ESInet and NGCS environment with zero service disruption. As detailed in the Sample Project Management Plan (Exhibit 4), our methodology follows a structured lifecycle:

- **Planning and Design:** Motorola initiates the project with a DDR to finalize system architecture, logical/physical topologies, and interconnection points. We collaborate with the State to integrate scheduling and coordination efforts into the master Project Management Plan.
- **Execution and Deployment:** Motorola manages all aspects of installation, including circuit provisioning, NGCS core functional element deployment, and GIS data synchronization. A dedicated Project Manager oversees the WBS to ensure all milestones are met.
- **Testing and Validation:** Before any PSAP migration, Motorola conducts rigorous Acceptance Test Plans (ATP) covering system reliability, security protocols, and failover capabilities. This ensures all components meet NENA i3 standards and State requirements.

- **Cutover and Transition:** We utilize a PSAP-by-PSAP work plan to manage the migration/cutover process. Each transition is supported by a 30-day reliability test to verify stability.
 - **Final Acceptance:** Motorola acknowledges that no service, system, or function is deemed Accepted until the State provides formal written approval following successful testing and confirmed cutover readiness.
-

b. Elements of Implementation

Provide a comprehensive implementation plan that addresses the full project lifecycle – from design and engineering through testing, training, and final system cutover – aligned with NENA Standards and industry best practices.

At a minimum, the implementation plan should address:

- Methodology for implementing the entire NG911 system, establishing call delivery from all OSPs to all PSAPs across the State of Nebraska.
- Methodology for administering and operating the NG911 system for the contract term.
- IP routing plan, how requirements are met, and governance of routing changes and documentation.
- How NGCS will operate with the ESInet, and how each Functional Element will deliver required functionality.

Motorola Response

Comply.

Motorola provides a comprehensive Sample Project Management Plan, detailed in Exhibit 4, that aligns with NENA i3 standards and industry best practices. Our methodology ensures a seamless transition for the State of Nebraska through the following elements:

- **End-to-End Implementation Methodology:** Motorola utilizes a phased approach to establish call delivery from all Originating Service Providers (OSPs) to every PSAP in Nebraska. This involves deploying LNG for legacy traffic and direct IP interconnections for modern providers. We manage the entire lifecycle from initial design and site surveys to final cutover, ensuring no loss of service during the migration.
- **Operational Methodology:** For the duration of the contract, Motorola will operate the NG9-1-1 system using a proactive service management framework. This includes 24/7/365 monitoring by our Network Service Operations Center (NSOC), routine maintenance, and adherence to strict SLAs to ensure system health and availability.
- **IP Routing and Governance:** Our IP routing plan is built on NENA i3 functional elements, including the ECRF and PRF. Motorola meets all state requirements by using geospatial data for precise call delivery. Any changes to routing logic are governed by a formal Change Management process, requiring State approval and immediate updates to the "as-built" documentation.

- **ESInet and NGCS Integration:** The NGCS operates as a suite of FEs hosted within the ESInet. Each element—such as the BCF for security and the Emergency Service Routing Proxy (ESRP) for call evaluation—works in concert to validate, route, and deliver emergency calls and data securely to the PSAP.
-

4. Transition

a. Transition Plan: Current and Future

This procurement may require transition from existing systems and/or services provided by the current service provider. The Respondent shall provide a **Transition Plan** ensuring services are not **diminished, interrupted, or disabled** and that **SLA metrics remain enforced** during transition.

Motorola Response

Comply.

Motorola provides a robust Transition Plan, further detailed in the Sample Project Management Plan Exhibit 4, designed to manage the migration from existing systems to the new ESInet and NGCS with zero service disruption. Our transition methodology centers on a "parallel operations" approach where the new infrastructure is fully tested and operational before any traffic is migrated away from legacy systems.

Key elements of our transition approach include:

- **Continuous Service Availability:** Motorola ensures that 9-1-1 services are never diminished or disabled during the transition. We maintain dual-path connectivity during the cutover phase to allow for immediate rollback should any issues arise.
 - **PSAP-by-PSAP Migration:** Transitions are executed according to a granular, PSAP-specific work plan. This allows for focused technical support and validation at each site, minimizing regional risk.
 - **SLA Enforcement:** All SLA metrics, including system uptime and call delivery performance, remain in full force throughout the transition period. Motorola's NSOC provides 24/7 monitoring to ensure performance standards are met during every phase of the migration.
 - **Carrier Coordination:** Motorola takes responsibility for coordinating with existing service providers and OSPs to manage the logical move of traffic to the new ESInet, ensuring a seamless handoff.
 - **Reliability Testing:** Following each PSAP cutover, a 30-day reliability period begins to verify system stability and performance before final formal acceptance.
-

Minimum topics:

- Transition schedule with milestone dates for design, development, testing, implementation, and cutover to full operational readiness.

- System testing approach during transition.
- PSAP/site cutover approach, including **phased migration** and **parallel operation** with current systems.
- **Contingency and rollback plan** for implementation or integration failures.
- Risks, dependencies, and interdependencies affecting cutover.
- **OSP interface** transition and service migration to the NG911 system.
- Integration with other systems, services, and providers.

Motorola Response

Comply.

Motorola's Transition Plan, outlined in the Sample Project Management Plan Exhibit 4, follows a structured methodology to move the State of Nebraska from legacy infrastructure to a NENA i3-compliant environment without service interruption.

- **Transition Schedule and Milestones:** The project schedule identifies specific dates for key milestones, including the DDR, core system development, rigorous functional testing, PSAP-by-PSAP implementation, and the final transition to full operational readiness.
- **System Testing Approach:** Before any live traffic migration, Motorola conducts comprehensive testing to validate the ESInet and NGCS. This includes connectivity testing, functional element validation, and end-to-end call flow verification to ensure the system meets all State requirements and NENA standards.
- **Cutover and Parallel Operation:** Motorola utilizes a phased migration strategy. The new NG9-1-1 system will operate in parallel with existing legacy services, allowing for thorough verification of the new path before the legacy connection is decommissioned.
- **Contingency and Rollback:** Each site-specific cutover includes a documented contingency plan. If a migration or integration failure occurs, Motorola maintains the ability to immediately roll back to the legacy environment, ensuring 9-1-1 service remains available at all times.
- **Risks and Dependencies:** Motorola actively manages a risk register that tracks dependencies, such as OSP readiness, circuit provisioning timelines, and GIS data maturity. We work closely with the State to mitigate these factors before they impact the cutover schedule.
- **OSP and Service Migration:** Motorola coordinates the transition OSP interfaces, utilizing LNGs where necessary to aggregate legacy traffic into the IP-based ESInet, ensuring a seamless migration of all emergency traffic.
- **System Integration:** Our approach includes formal integration planning with third-party providers and existing State services. We ensure all interfaces—including NNI connections to neighboring regions—are tested and validated for interoperability.

Responsibilities: If a new provider is selected, the Contractor must engage the current provider and coordinate the transition. If a transition **away** from the Contractor's system is required later (including contract expiration), the Contractor shall cooperatively plan and execute the transition. Current 911 call delivery, features, functions, capabilities, and operations **must not be limited or impacted** by the proposed solution.

Motorola Response

Comply.

5. Testing and Acceptance

a. Testing (Comprehensive Test Plan)

System testing is required **before acceptance** of any component or function **and before cutover** to full operational status and commencement of payment. With the proposal, provide an **example NG911 System Test Plan** covering each element of the proposed system. Post-award, the test plan must be submitted to the State for approval at least thirty (30) days prior to the start of testing of any system function or components.

The comprehensive test plan will address, at minimum:

- Test environment, facilities, and equipment.
- Test configurations and thresholds.
- Simulators and test-call processes.
- Final documentation of all tests and results.

Motorola Response

Comply.

Motorola requires comprehensive system testing and formal State approval before the acceptance of any component, function, or the commencement of billing. Our testing methodology ensures that the Nebraska ESInet and NGCS meet all NENA i3 standards and State-specific requirements. Descriptions of the **NG9-1-1 System Test Plan** are provided in the Preliminary Project Management Plan Exhibit 4, which serves as the foundation for the final customized plan.

Post-award, Motorola will submit the finalized test plan to the State for approval at least 30 days prior to the start of any testing activities. At a minimum, this plan addresses:

- **Test Environment and Facilities:** Motorola establishes a dedicated test environment that mirrors the production architecture. This includes the necessary core FEs, network termination points, and monitoring tools to validate system performance without impacting live emergency traffic.
- **Configurations and Thresholds:** The plan defines the specific configuration parameters for each functional element (e.g., BCF, ESRP, ECRF). We establish performance thresholds for call setup times, media quality, and failover triggers to ensure the system operates within defined SLAs.
- **Simulators and Test-Call Processes:** Motorola utilizes industry-standard call simulators and structured test-call procedures. This includes generating various call types (Wireline, Wireless, VoIP, Text-to-911) and simulating peak traffic loads—up to 200% of historical peaks—to verify system stability and routing accuracy.

- **Final Documentation and Results:** Upon completion of each testing phase, Motorola provides comprehensive documentation of all results. This includes detailed logs, pass/fail status for each test case, and a formal record of any remediation steps taken. Final system acceptance is contingent upon the State's written approval of these results.
-

System Testing must address, at minimum:

- NENA-STA-010.3 Functional Element testing.911 call flow: primary, alternate, last route.
- End-to-end traffic flow.
- Functional Element ↔ Functional Element tests.
- Protocol ↔ Protocol tests.
- Port ↔ Port tests.
- Load testing: unexpected surge, short burst, sustained overflow.
- ESInet throughput and capacity.
- ESInet end-to-end connectivity (fault tolerance, failover, alternate routing, monitoring systems, fault notification).
- Security controls: firewalls, intrusion detection systems, intrusion prevention systems.
- Throughput acceptance testing of ≥24 hours, simulating 200% peak traffic load.

Motorola Response

Comply.

State participation and rights: Share results with the project team prior to acceptance; the State may require re-tests and may assign observers. The State may inspect test equipment and/or applications and must approve remediation actions from failed tests.

Motorola Response

Comply.

b. Test Plan Methodology

Describe the methodology for testing all NG911 system components, including those provided by Subcontractors or other suppliers, addressing the coverage area in §C-5.a. (Testing). Include regression testing procedures following defect remediation.

Motorola Response

Comply.

Motorola utilizes a structured testing methodology to validate all ESInet and NGCS components, including those from third-party suppliers, ensuring full coverage of the Nebraska service area. Our

approach integrates individual component validation with end-to-end system testing to ensure NENA i3 compliance and operational readiness.

Testing Methodology

Motorola's methodology encompasses the following phases to ensure comprehensive coverage:

- **Component and Supplier Testing:** Every functional element and network component, regardless of the supplier, undergoes standalone validation to ensure it meets technical specifications and security requirements before integration.
- **Integration Testing:** We verify the seamless interoperability between different FEs (e.g., ESRP to ECRF) and across the ESInet to ensure that call signaling and media flows correctly across the entire architecture.
- **End-to-End System Testing:** Motorola conducts comprehensive call flow testing from OSP ingress points to final PSAP delivery, validating primary, alternate, and default routing scenarios.
- **Reliability and Load Testing:** The system is subjected to high-volume traffic simulations—including 200% peak load tests over 24 hours—to ensure stability and throughput capacity across the state's coverage area.

Regression Testing and Defect Remediation

To maintain system integrity following any identified issues, Motorola employs a rigorous remediation and regression process:

- **Defect Remediation:** When a test failure occurs, the issue is logged, analyzed, and corrected by the appropriate technical team or subcontractor.
 - **Regression Testing Procedures:** Once a defect is remediated, Motorola performs targeted regression testing to confirm the fix is successful and ensure the change has not introduced new issues into previously validated functions.
 - **Verification and Re-Acceptance:** After successful regression testing, the specific test case is repeated in the presence of State observers, if required, to secure formal approval and move the component back into the acceptance lifecycle.
-

c. System Acceptance Testing

Acceptance testing must be completed prior to the State's final acceptance of the system. Final certification and system acceptance occurs **only after** the Contractor has provided acceptance test results to the State **and** the State has certified that the testing satisfactorily meets all requirements.

Motorola Response

Comply.

The Respondent must describe their approach for documenting the test results and may use the following codes to discuss their methodology:

- TP – Test Passed
- TF – Test Failed
- RTP – Retest Passed
- RTF – Retest Failed
- NA – Feature not applicable to the final configuration

On any failure the Contractor shall correct the deficit and perform regression testing to re-validate and re-certify all affected tests. Results of failed tests shall be documented and presented in writing to the State. Successful regression testing results must be delivered to the State

Motorola Response

Comply.

Motorola utilizes a structured and transparent methodology for documenting all test results throughout the Nebraska ESInet and NGCS implementation. Each test case identified in the System Test Plan is tracked in a master Test Results Matrix, ensuring the State has a clear audit trail of system performance and compliance.

Documentation Methodology and Status Codes

To provide clarity and consistency, Motorola uses the following standardized status codes to track the lifecycle of every requirement:

- **TP – Test Passed:** The component or function met all defined criteria on the first attempt.
- **TF – Test Failed:** The test did not meet the required threshold or functional outcome.
- **RTP – Retest Passed:** Following successful remediation of a **TF** result, the feature was re-tested and is now verified as passing.
- **RTF – Retest Failed:** The feature failed again after a remediation attempt, triggering immediate technical escalation.
- **NA – Feature Not Applicable:** The test case is not relevant to the final configuration approved for the State.

Deficit Correction and Regression Testing

Motorola maintains a rigorous process for handling any Test Failed (**TF**) to ensure system integrity is never compromised:

- **Written Notification:** Results of all failed tests are documented and presented in writing to the State, including a preliminary root cause analysis.
- **Deficit Correction:** Motorola technical teams will correct the identified deficit.
- **Mandatory Regression Testing:** Once a fix is implemented, Motorola performs regression testing to re-validate the specific feature and re-certify all affected system functions. This ensures that the remediation did not inadvertently impact other parts of the NG9-1-1 environment.

- **Verification Delivery:** Successful Regression Testing Results (**RTP**) must be delivered to the State for review. Final system acceptance is contingent upon all critical functions achieving a **TP** or **RTP** status.
-

d. Independent Validation and Verification (IV&V)

Upon acceptance, the State will conduct IV&V testing using a third party. The Contractor shall collaborate to establish IV&V scope and priorities and support execution.

The Respondent **MUST** state acceptance of third-party IV&V testing of all elements required in this procurement document in its response to this RFP.

Motorola Response

Comply.

Motorola hereby states its full acceptance of third-party IV&V testing for all elements, systems, and services required under this procurement.

Section 4

Deliverables and Deliverable Approval Process

The PSC and the State recognize that the Contractor is responsible for end-to-end traffic from caller to call-taker. This includes the OSP ingress to the point(s) of interconnection (POI) and the delivery from the ESInet to the PSAP's call handling equipment (CHE).

The Contractor is responsible for all requirements in this RFP, including providing a comprehensive risk assessment of administrative, operational, and technical factors that could prevent achievement of the 99.999% availability service level for the end-to-end system. The assessment must identify, at a minimum, areas with limited physical diversity, underestimated redundancy, or single-threaded network resources, and propose mitigation for each.

Motorola Response

Comply.

1. ESInet Architecture and Design :

System Requirements

Deliver a managed IP-based ESInet conforming to NENA i3 architecture, supporting legacy PSTN and SIP call flow, IPv4/IPv6 addressing, QoS mechanisms (e.g., DiffServ), and traffic segregation. Ensure no single point of failure through diverse network paths for the entire system, redundant nodes and functional elements, redundant data centers, and automatic failover (RPO <1 minute, RTO <5 seconds). Provide scalable bandwidth with traffic shaping and congestion management.

Deliverables:

- Detailed network architecture diagrams including IP addressing, VLANs, QoS policies, diversity topology, and redundancy model.
- Demonstration of SIP TLS and SRTP call signaling, media traversal with zero packet loss during failover.
- Documented RTO RPO targets, MTTR SLAs (<2 hours for critical issues), and failure mode analysis reports.

Motorola Response

Comply.

Per the instructions in this section, upon award, Motorola will provide these deliverables.

2. NG911 Core Services (NGCS)

System Requirements:

Supply or interoperate with NGCS components (BCF, LVF, LIS, ECRF, ESRP, PRF, LNG) per NENA standards, supporting SIP interfaces to all interconnections, PIDF-LO, and HELD protocols. Ensure performance (e.g., 200 millisecond median lookup latency, 10 queries per second), scalability for peak loads, and isolation capabilities. Log all transactions with timestamps, correlation IDs, and searchable storage.

Deliverables:

- Provide a mapping / traceability document aligning proposed system and service modules to NGCS functions and interface conformance statements.
- Interoperability test results with SIP calls and packet traces.
- Performance test results and scalability benchmarks.

Motorola Response

Comply.

Per the instructions in this section, upon award, Motorola will provide these deliverables.

3. GIS and Location-Based Routing

System Requirements:

Implement NENA-compliant GIS data model NENA-STA-006.2-2022 for ECRF/LVF, supporting civic/geodetic location validation and routing. Use PIDF-LO for location transport, enable push pull delivery to PSAPs, and support Policy-based routing (with PRF) with alternate routing logic. Provide GIS data versioning, automated updates, and provisioning APIs.

Deliverables:

- GIS data model documentation, sample datasets, and entity-relationship diagrams.
- Demonstration of location-based routing to the correct PSAP mapping for civic geodetic inputs, including edge cases.
- GIS update procedures and API specifications.

Motorola Response

Comply.

Per the instructions in this section, upon award, Motorola will provide these deliverables.

4. Security, Privacy, and Trust

System Requirements:

Implement NENA NG-SEC model with mutual TLS, RBAC, MFA, and encryption (TLS 1.3, AES-256). Mitigate DDoS/TDoS/SIP attacks via rate limiting and anomaly detection and blocking, isolation when necessary. Manage certificates, and provide incident response plans, vulnerability management, and SIEM integration.

Deliverables:

- Security architecture diagrams, PKI policies, RBAC matrices, and access control configurations.
- Recent penetration test reports and SLAs for patching.
- Demonstration of mutual TLS, anomaly detection, and SIEM log integration.

Motorola Response

Comply.

Per the instructions in this section, upon award, Motorola will provide these deliverables.

5. Logging, Reporting, and Call Detail Records

System Requirements:

Log all ESInet NGCS events with timestamps, correlation IDs, and tamper-evident mechanisms. Generate NENA compliant CDRs capturing call details to deliver to the Statewide reporting system. Retain logs' CDRs for a defined period of time (which may be different for each jurisdiction) with secure, searchable storage.

Deliverables:

- Sample logs, CDR schemas, retention procedures, and RBAC policies.
- Demonstration of CDR generation, search/export, and operational reports.
- Evidence of tamper-evident storage and audit trails for admin changes.

Motorola Response

Comply.

Per the instructions in this section, upon award, Motorola will provide these deliverables.

6. Interoperability, Testing, Conformance, and System Acceptance

System Requirements:

Demonstrate NENA i3 conformance via self-attestation and multi-vendor interoperability tests. Conduct phased testing (unit, integration, failover, performance at 150% capacity, security) with 100% pass rates for critical flows. Provide comprehensive documentation and training.

Deliverables:

- Test plans, conformance matrices, and interoperability test schedules.
- Pilot lab demonstration with KPIs (e.g., 99.999% uptime).
- User manuals, API specs, and training curricula.

Motorola Response

Comply.

Per the instructions in this section, upon award, Motorola will provide these deliverables.

7. Operational Support and Service Level Agreements (SLAs)

System Requirements:

Commit to SLAs (99.999% availability, <2-hour MTTR for Priority 1 issues, 15-minute acknowledgment). Provide training, runbooks, and documentation using NENA terminology. Implement change management with maintenance windows, rollback procedures, and 30-day notifications.

Deliverables:

- SLA documents, training curricula, sample runbooks, and maintenance calendar.
- References from three comparable NG911 deployments with uptime reports.

- System and Service provided must be delivered compliant with NENA standards at acceptance unless mutually agreed upon provisions are acceptable. In this event, the contractor must provide a plan, timeline and communicate regularly with the State and the Advisory Committee on progress to full NENA standard conformance.
- Furthermore, as Standards evolve the contractor **MUST MAINTAIN** conformance with any new revisions to standards listed as requirements in this RFP. The State will allow a period of 9 months for the contractor to become compliant as a guideline. It is incumbent on the contractor to identify any areas they may be unable to meet the 9-month target and produce a plan and timeline to achieve conformance.

Motorola Response

Comply.

Per the instructions in this section, upon award, Motorola will provide these deliverables.

Submission Requirements

- Respondents must provide a written reply for each requirement within this RFP with descriptions of their proposed system (unless otherwise noted) and services to meet or exceed the requirement. If a requirement is not fully met, an exception can be made but any exception must include an alternative. If a requirement is on a roadmap for future implementation that must be clearly identified with a timeline that shows when deployment is expected.
- Provide a detailed project plan, including timelines, milestones, and resources for deployment, testing, and ongoing support.
- Submit all deliverables in electronic format, including architecture diagrams, test reports, sample logs, and documentation.

Motorola Response

Comply.

Deliverables are subject to the Deliverable Approval Process, contained in the terms and conditions.

Motorola Response

Comply.

Section 5

Technical Requirements

1. ESInet Requirements

The Emergency Services IP Network (ESInet) must comply with NENA-STA-010.3-2021 (i3 Standard) and follow the recommendations in the NENA Emergency Services IP Network Design (ESIND) Information Document (NENA-INF-016.2-2018). The ESInet shall interconnect all NG911 components with Public Safety Answering Points (PSAPs) and OSPs using Internet Protocol (IP), and, where necessary, legacy methods.

Motorola Response

Comply.

Motorola complies with the latest i3 version NENA-STA-010.3f-2021 and NENA-INF-016.2-2018.

The Respondent shall provide an ESInet design that conforms to the NENA i3 architecture for a managed IP-based emergency services network. The design shall support multi-tenant interconnects with the Public Switched Telephone Network (PSTN) and Session Initiation Protocol (SIP), diverse physical routing paths, and network-level redundancy that eliminates any single point of failure. The ESInet must natively support IPv4 and IPv6, implement Quality of Service (QoS) to prioritize emergency traffic, and use virtual routing or equivalent technologies to segregate emergency services traffic from non-emergency traffic. The design shall include scalable bandwidth to handle peak loads, with automatic traffic shaping and congestion management.

Motorola Response

Comply.

The ESInet shall support SIP per **RFC 3261** and applicable NG911 SIP extensions, including SIP over **Transport Layer Security (TLS)** for signaling and **Secure Real-time Transport Protocol (SRTP)** for media. Standard transports, including full IPv6 compatibility shall be supported, including TLS over TCP, and UDP where applicable. Interfaces must support both location-by-reference and location-by-value conveyance to ensure seamless integration with OSPs.

Motorola Response

Comply.

The ESInet shall support standard cross-connect and peering arrangements, selective routing, and boundary elements such as **Border Control Functions (BCFs)**. **Border Gateway Protocol**

(BGP) shall be used for multi-site reachability and load distribution. The Respondent shall provide documented procedures, application programming interfaces (APIs), and configuration templates for peering with adjacent ESInets, third-party providers, and legacy networks, including policy-based routing and traffic-exchange agreements.

Motorola Response

Comply.

The ESInet shall incorporate geographically diverse, redundant network cores; duplicate session border/edge elements; and automatic, transparent failover for signaling and media so that failure of any single component (e.g., link, router, or server) does not disrupt 911 service. The Respondent shall define and guarantee a **Recovery Point Objective (RPO)** of less than one (1) minute and a **Recovery Time Objective (RTO)** of less than five (5) seconds for critical paths, with active-active or active-passive configurations across data centers separated by at least 100 miles.

Motorola Response

Comply.

The ESInet shall enforce Differentiated Services (DiffServ) or equivalent QoS policies to prioritize 911 signaling (for example, SIP INVITE transactions) and media streams, with configurable DSCP markings. It must support bandwidth provisioning, traffic policing, and shaping to maintain PSAP-grade voice quality (Mean Opinion Score [MOS] greater than 4.0) and data integrity under load, including mechanisms to handle burst traffic and to prevent overload.

Motorola Response

Comply.

The Respondent shall supply a comprehensive **Network Management System (NMS)** or **Element Management System (EMS)** with real-time dashboards; syslog export; SNMPv3 polling and traps; and key performance indicators (KPIs) including latency, packet loss, jitter, and utilization, aligned with NENA operational guidance. The system must provide threshold-based alerting, historical trend analysis, and integration with external tools via APIs.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section, including a clear description of:

- Network operations management (operational policies, staffing, incident response, and system management procedures).

Motorola Response

Comply.

1. Operational Policies

Motorola operates a 24x7 NSOC providing continuous monitoring and support for NG9-1-1 and ESInet services. Operations align with applicable policies, NENA i3 standards, NIST cybersecurity guidance, and applicable CJIS requirements. Standard ITIL-based processes govern incident management, change control, configuration management, and service reporting. All operational activities are logged, auditable, and reviewed for continuous improvement.

2. Staffing

The Motorola NSOC is staffed 24x7x365 with trained network, systems, and public-safety support personnel. Staffing includes Tier 1 monitoring analysts, Tier 2/3 network and systems engineers, cybersecurity specialists, and an on-call Incident Manager. Personnel supporting Nebraska NG9-1-1 services are trained on ESInet architecture, PSAP operations, vendor interconnections, and public safety availability requirements.

3. Incident Response Procedures

Motorola uses a standardized incident response process with defined severity levels (P1–P4). Incidents are detected via automated monitoring, PSAP reports, carrier notifications, or cybersecurity alerts. P1 and P2 incidents impacting call delivery or PSAP access trigger immediate NSOC response and notification to NSOC within 10 minutes. Motorola coordinate's fault isolation, failover, vendor engagement, and service restoration, providing status updates every 30 minutes until resolution. Root cause analysis and corrective action reports are delivered within two business days.

4. System Management Procedures

Motorola manages NG9-1-1 and ESInet systems through formal change, configuration, and security management processes. All changes are risk-assessed, approved, scheduled, and documented with rollback plans. System performance, availability, and security are continuously monitored. Backup, redundancy, and disaster recovery capabilities are tested regularly to ensure high availability of public safety services. Operational metrics, including availability, MTTR, and SLA compliance, are reported to the Commission on a recurring basis.

-
- Detailed physical and logical security measures (encryption protocols, access controls, secure access points, and physical security for data centers); strategies for achieving 99.999% uptime with contingency plans.

Motorola Response

Comply.

1. Physical and Logical Security Measures (NENA i3 Compliant)

Physical Security: Data centers hosting NG9-1-1 i3 FEs comply with NENA i3 availability and resiliency expectations. Facilities provide 24x7 security staffing, controlled access using badge and biometric authentication, video surveillance, visitor logging, and redundant power, HVAC, fire

suppression, and environmental controls. Geographic diversity is implemented to support i3-required service continuity.

Logical Security & Access Controls: Logical protections align with NENA i3 cybersecurity principles for ESInets. Role-based access control, least-privilege enforcement, and multi-factor authentication protect i3 FEs, management systems, and signaling networks. Network segmentation separates i3 core services, management planes, and external interconnections, including OSPs and PSAPs. Secure administrative access is provided through hardened jump hosts and monitored VPN gateways.

Encryption Protocols: Consistent with NENA i3 security recommendations, SIP signaling, web services, and management traffic are encrypted using TLS 1.2/1.3, while IPsec is used for ESInet inter-site and carrier connections where applicable. Data at rest supporting i3 services is encrypted using AES-256 or equivalent. Cryptographic key management follows NIST guidance referenced by NENA i3.

2. NENA i3–Based 99.999% Availability Strategy

Motorola's ESInet architecture supports NENA i3 requirements for resiliency by deploying i3 FEs in active-active configurations across geographically separated locations. Core i3 services such as ECRF, LVF, ESRP, and logging services are designed without single points of failure. Dynamic routing, load balancing, and automated failover ensure uninterrupted call routing and data delivery during infrastructure, carrier, or site outages.

3. Contingency and Continuity Planning Under NENA i3

Failover and Rerouting: In accordance with NENA i3 call processing principles, calls and associated data are automatically rerouted to alternate PSAPs or processing elements during outages.

Disaster Recovery: Near-real-time replication of i3 service data supports rapid restoration while maintaining call integrity and auditability.

Testing and Validation: High-availability, failover, and cybersecurity controls are regularly tested against NENA i3 operational expectations. Results are documented, reviewed with stakeholders, and used to continuously improve NG9-1-1 service reliability.

-
- Continuous performance monitoring mechanisms with logging and alert systems; real-time alarm generation and notification strategies.

Motorola Response

Comply.

Motorola's NSOC uses **continuous performance monitoring** across all NG9-1-1 and ESInet components, including i3 FEs, network infrastructure, cybersecurity controls, and application services. Centralized logging collects system, security, and application logs in real time and retains them per NENA i3 and State requirements. Logs are correlated to identify performance degradation, security events, and service anomalies, supporting rapid troubleshooting and auditability.

Real-time alarms and notifications are generated through automated thresholds and event correlation for call failures, latency, packet loss, service unavailability, and security indicators. Alerts are prioritized by impact (P1–P4) and immediately routed to the Motorola NSOC via dashboards, paging,

and secure messaging. P1/P2 alarms trigger immediate operator action and customer notification per SLA, ensuring rapid response to any condition affecting NG9-1-1 service availability.

- Guidelines for routine, updates, and emergency maintenance; comprehensive disaster recovery plan with RTO and RPO details.

Motorola Response

Comply.

Our formal maintenance guidelines are aligned with ITIL and NENA i3. Routine maintenance includes health checks, patch validation, backups, and performance tuning, and is performed during approved maintenance windows with advance notice to the Commission. Planned updates follow documented change management with risk assessment, testing, approval, and rollback plans. Emergency maintenance is executed immediately when required to protect NG9-1-1 availability or security, with rapid notification to the Commission and post-maintenance reporting.

We maintain a comprehensive DR plan for NG9-1-1 and ESInet services using geographically diverse, active-active sites with continuous data replication. **RTO** for critical call-handling and routing services is near-zero to minutes, achieved through automated failover. **RPO** is near-zero due to real-time replication of operational data and logs. DR procedures are tested regularly, documented, and reviewed to ensure sustained 99.999% operational availability.

- Procedures for service restoration post-incident.

Motorola Response

Comply.

We follow a structured service restoration process to rapidly and safely return NG9-1-1 and ESInet services to full operation. Upon stabilization of the incident, our NSOC engineers validate system integrity, confirm call routing and data flows, and coordinate with carriers and affected PSAPs to verify end-to-end functionality. Temporary fixes are replaced with permanent corrections using approved change procedures, and all systems are returned to normal operating modes.

After **restoration**, our NSOC completes a **post-incident** process that includes customer confirmation, incident closure, and delivery of a root cause analysis with corrective and preventive actions. System performance is closely monitored for a defined period to ensure stability, and lessons learned are incorporated into operational procedures to prevent recurrence.

- Proactive outage prevention and response strategies including redundancy testing.

Motorola Response

Comply.

We employ **proactive outage prevention** and **response strategies** aligned with NENA i3 resiliency principles to protect our NG9-1-1 and ESInet services. Continuous monitoring, capacity management, and trend analysis identify risks before service impact occurs. i3 FEs are deployed with no single point of failure using active-active architectures, diverse routing, and redundant carriers. Configuration baselines and security controls are regularly reviewed to prevent degradation or misconfiguration.

Response and **redundancy testing** are integral to operations. Automated failover and call rerouting are triggered immediately upon fault detection, consistent with i3 call processing requirements. Redundancy, failover, and DR tests are conducted on a scheduled basis and after significant changes to validate ESRP, ECRF, LVF, and logging service resiliency. Test results are documented, reviewed with stakeholders, and used to continuously improve NG9-1-1 availability.

- Technical specifications for core routing architecture with diverse paths and load balancing.

Motorola Response

Comply.

Our proposed NGCS core routing architecture for the Commission is designed to meet NENA i3 requirements for resiliency, diversity, and call continuity. Our core routing solution uses multiple geographically separated, active-active ESRPs connected through diverse physical paths, carriers, and network providers to eliminate single points of failure. Dynamic routing protocols and policy-based routing ensure uninterrupted call delivery between origination networks and PSAPs.

Load balancing and traffic management are implemented across our i3 Functional Elements to distribute call signaling and data traffic based on health, capacity, and latency. Automated health checks remove failed components from service and redirect traffic in real time. Our architecture supports seamless failover, call rerouting, and sustained performance during peak loads or infrastructure outages, consistent with NENA i3 call processing and ESInet design principles.

- Interfaces with hosted solutions or third-party providers.

Motorola Response

Comply.

The proposed ESInet complies with NENA i3 standards and is implemented as an open, interoperable architecture. We support standardized NENA i3 SIP interfaces and REST/JSON APIs to enable seamless integration with third-party hosted systems, including external GIS data sources, supplemental data providers and adjacent regional ESInets.

Interconnection security is enforced through a NENA i3-compliant BCF. The BCF supports secure connectivity using private peering or VPNs and applies mutual TLS (mTLS) for authentication and trust between the Nebraska ESInet core and all external entities.

- Fault zone design methodology identifying critical components and failure points.

Motorola Response

Comply.

Our fault zone design methodology follows NENA i3 best practices that segment the network into independent operational enclaves. Critical components, including ESRP routing services, ECRF location services, SIP core elements, BCF, and database layers, are clustered within each fault zone so failures are contained and do not cascade across the ESInet.

Each of the zones is deployed with geographic and logical diversity, redundant power, compute, and network paths, and active-active service instances. Specific failure scenarios, such as a memory leak in an individual ECRF node, are isolated within the zone through clustering and automatic failover. Identified high-risk failure points, including the Point of Interconnection (POI) and PSAP demarcation point, are mitigated using diverse dual-entrance fiber paths (where available) and redundant edge gateways, ensuring continuous service availability.

- Bandwidth management protocols prioritizing emergency traffic.

Motorola Response

Comply.

Our bandwidth management is enforced through a strict QoS and DiffServ hierarchy aligned with NENA i3 standards. Real-time emergency voice and media are marked with DSCP 46 (Expedited Forwarding), while SIP signaling is marked with DSCP 24 (Assured Forwarding) to ensure proper call setup and control.

This traffic prioritization strategy guarantees that 9-1-1 traffic preempts all non-critical data, including GIS updates and administrative traffic, at the router and transport levels. The result is consistent, public-safety-grade call quality, and media delivery even during periods of network congestion.

Our bandwidth management and traffic prioritization approach are driven primarily by NENA STA-010.3f (NENA i3 Standard for Next Generation 9-1-1). This standard defines IP-based call handling, the use of QoS and DiffServ mechanisms, and the prioritization of real-time emergency voice, video, and signaling traffic over non-critical data.

- And any bandwidth sharing arrangements with implications for priority traffic.

Motorola Response

Comply.

Our proposed ESInet is governed by strict Traffic Shaping and Policing policies. These arrangements guarantee a "Committed Information Rate" (CIR) specifically for 9-1-1 traffic, ensuring that non-emergency data sharing between agencies cannot impede the priority flow of emergency calls.

Additionally, we use a controlled bandwidth-sharing model that allows non-emergency and supported traffic to utilize available capacity without impacting 9-1-1 services. All shared links are governed by NENA i3-aligned QoS and DiffServ policies, with emergency voice and media assigned the highest priority and guaranteed bandwidth.

During congestion, priority queuing and traffic preemption ensure that 9-1-1 call signaling and media are preserved while lower-priority traffic is delayed or dropped. This approach enables efficient use of network capacity while maintaining public-safety-grade performance for all emergency communications.

- Any limitations in the “span of control” over connections to the OSPs or PSAPs that are linked to the ESInet to establish a risk register for future reference.

Motorola Response

Comply.

Any identified limitations associated with the “span of control” over connections to the OSPs or PSAPs will be documented in a project risk register for future reference.

Additionally, the Respondent must investigate and document potential single points of failure, explain detection and activation of standby systems if not active-active, and detail ESInet interconnection points with OSPs and PSAPs for full IP-based NG911 functionality.

Motorola Response

Comply.

Our proposed service is designed for high availability with no single points of failure utilizing an Active/Active architecture. Network traffic is load-balanced across redundant hardware, software, and geographically diverse IP network routes. Interconnection points with OSPs are redundant and diverse interfacing with redundant instances of LNGs and BCFs. The ESInet terminating at the call handling system host locations leverages an SDWAN architecture terminating on redundant SDWAN edge appliances.

1.1 Architecture and Topology

1.1.1 ESInet Diagrams

The contractor must submit comprehensive diagrams that visually represent the proposed ESInet architecture. These diagrams must be kept current and be included in a configuration management database that the 911 Advisory Committee and the State may access at any time during the contract to validate the deployment and system functionality.

Motorola Response

Comply.

The diagrams associated with the proposed architecture are provided in Exhibit 6 Architecture and Topology Diagram.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Comprehensive diagrams illustrating network maps (logical and physical topologies).

Motorola Response

Comply.

In accordance with this requirement, comprehensive network diagrams illustrating the service architecture are provided in Exhibit 6 Architecture and Topology Diagram. These diagrams detail the highly available, geo-redundant design of our Next Generation 9-1-1 (NG9-1-1) solution.

The provided documentation includes:

- **Logical Topology Diagrams:** These illustrate the NENA i3-compliant architecture, data flows, and SIP signaling paths. They show the secure interaction between all NGCS functional elements, including the BCF, Emergency Services Routing Proxy (ESRP), ECRF, and LVF, across our active-active, multi-cloud environment.
 - **Physical Topology Diagrams:** These detail the physical hardware deployments, geo-diverse data center locations, and carrier-diverse transport paths. They visually show the physical "last mile" connectivity from OSP Points of Interconnection (POIs), through the ESInet, down to the physical demarcation points at each PSAP facility.
-

- Physical and logical path diversity for redundancy.

Motorola Response

Comply.

In accordance with this requirement, the comprehensive network diagrams illustrating the redundant design of our Next Generation 9-1-1 (NG9-1-1) architecture are provided in Exhibit 6 Architecture and Topology Diagram]. These diagrams demonstrate how our service is engineered to deliver up to 99.999% Operational Availability by eliminating single points of failure across both physical and logical layers.

The provided documentation includes:

- **Physical Topology Diagrams (Physical Diversity):** These diagrams detail the geographic separation of our service across facilities. They visually map the carrier-diverse national networks, as well as the physically diverse "last mile" transport circuits, the Points of Interconnection (POIs), and PSAP demarcation points.
 - **Logical Topology Diagrams (Logical Diversity):** These diagrams illustrate our active-active, multi-cloud architecture. They map the NENA i3-compliant data flows, demonstrating how the Emergency Services Routing Proxy (ESRP) and PRF instantly and automatically steer SIP traffic over alternate logical paths if a disruption is detected, all without human intervention.
-

- One-time and transitional network elements.

Motorola Response

Comply.

In accordance with this requirement, comprehensive network diagrams illustrating the transitional phases of our service deployment are provided in Exhibit 6 Architecture and Topology Diagram. We recognize that the migration to a fully native IP architecture is a phased process, and these diagrams detail the specific elements deployed to bridge legacy and modern networks.

The provided documentation includes visual representations of the following transitional elements:

- **Legacy Network Gateways (LNGs):** The diagrams illustrate how legacy Time Division Multiplexing (TDM) and analog traffic from OSPs is ingested at the POI. The diagrams show the LNGs acting as transitional bridges, utilizing Protocol Interworking Functions (PIFs) to convert legacy voice traffic into i3-compliant SIP messaging before entering the ESInet.
 - **Legacy Selective Router Gateways (LSRGs):** Topologies showing the deployment of LSRGs to maintain critical voice and transfer connectivity with neighboring jurisdictions or downstream PSAPs that may still be operating on legacy selective routers.
 - **Phased Migration Paths:** Logical diagrams demonstrating the lifecycle of these one-time elements, illustrating how LNGs and LSRGs are gradually bypassed or decommissioned as OSPs and neighboring jurisdictions upgrade to native SIP interconnectivity.
-

- Network ingress and egress points with connections to OSPs, PSAPs, and external interfaces.

Motorola Response

Comply.

In accordance with this requirement, comprehensive network diagrams illustrating the boundary flows of our Next Generation 9-1-1 (NG9-1-1) architecture are provided in Exhibit 6 Architecture and Topology Diagram. These diagrams provide a detailed visual diagram of how traffic securely enters, traverses, and exits the Service.

The provided documentation includes specific illustrations of the following:

- **Network Ingress & OSP Connections:** The diagrams detail the Points of Interconnection (POIs) where OSPs hand off 9-1-1 traffic. This includes native IP connections passing directly through the BCF via Session Border Controllers (SBCs), as well as legacy TDM/analog traffic entering through Legacy Network Gateways (LNGs) for SIP conversion prior to ESInet routing.
 - **Network Egress & PSAP Connections:** The diagrams illustrate the egress paths from the ESInet down to each PSAP Hosts. This details the physical and logical demarcation points, the delivery of SIP traffic to i3-compliant CPE.
 - **External Interfaces:** The logical topologies highlight secure connections to critical external systems outside the core call-routing flow. This includes interfaces with Location Information Servers (LIS), external GIS authorities for the LVF, and secure gateways for transferring calls and data to neighboring regional or state ESInets.
-

- Transport types (e.g., MPLS or Ethernet) with port speeds.

Motorola Response

Comply.

Our Service utilizes highly reliable, standards-based transport technologies engineered to support secure, low-latency IP routing while ensuring strict QoS for mission-critical voice and data traffic.

- **Core ESInet Transport:** Our service utilizes national and regional backbones for our ESInet leveraging highly resilient, carrier-diverse networks. The ESInet provides the necessary traffic engineering, prioritization, and secure private routing required to isolate 9-1-1 traffic from the public internet. Core network node connections typically utilize high-capacity ports scaling from 10 Mbps to 500 Mbps access capacity engineered to handle aggregated statewide or regional traffic volumes seamlessly.
 - **Last-Mile and PSAP Transport:** For "last-mile" connectivity extending from the core ESInet to the PSAP Host demarcation points, we provision multiple circuit technologies using Software-Defined Wide Area Network (SD-WAN) overlay to provide a robust network eliminating single points of failure.
 - **Scalable Port Speeds:** PSAP Hosts and local POI port speeds are scalable based on concurrent call volume, multimedia payload requirements, and jurisdiction size. Standard edge deployments typically range from 10 Mbps to 100 Mbps for smaller or transitional sites, up to 500 Mbps for large PSAP Hosts natively ingesting IP data and rich multimedia.
-

- Capacities and estimated bandwidth at ingress, core, and egress points

Motorola Response

Comply.

Our service is engineered to provide highly scalable, non-blocking network capacities designed to handle both current mission-critical voice traffic and the future influx of rich multimedia (e.g., text, photo, and video). Bandwidth at each network segment is continuously monitored and scalable:

- **Ingress Points (POIs):** At the Points of Interconnection where traffic from OSPs enters the network, we provision high-capacity, redundant connections. The ingress port speed of 1 Gbps capacity is engineered to seamlessly absorb aggregated regional call volumes and provides massive overhead to mitigate sudden volumetric traffic spikes or DDoS attempts at the network edge.
- **Core Network (ESInet Backbone):** The regional and national backbone connecting our active-active routing engines and NGCS operates on extremely high-capacity transport. Core links range from 10 Mbps to 500 Mbps. This capacity ensures ultra-low-latency synchronization and provides seamless, bottleneck-free traffic failover between regions during a disruption.
- **Egress Points (PSAPs):** Bandwidth at the egress points, terminating at the local PSAP Host demarcation points, are engineered based on the agency's size, concurrent call-taker positions, and expected multimedia loads.
 - **Small to Medium PSAP Hosts:** Typically provisioned with redundant 10 Mbps to 100 Mbps circuits, providing ample bandwidth for SIP voice and basic NG9-1-1 data sets.

- **Large PSAP Hosts:** Typically provisioned with redundant 100 Mbps to 500 Mbps circuits to support high concurrent call volumes, and heavy video-to-911 payloads without impacting voice QoS.
-

- Interconnection locations (nodes, data centers, POIs, LRGs); and any additional technologies and interfaces.

Motorola Response

Comply.

Our service is distributed across highly secure, geographically diverse locations to ensure localized survivability and nationwide resilience. The system architecture includes the following interconnection points and interfaces:

Interconnection Locations

- **Core Data Centers:** The NGCS routing services are distributed across geographically diverse facilities and multi-cloud environments to ensure national resilience.
- **Points of Interconnection (POIs):** Redundant ingress points deployed within designated access areas where OSPs securely hand off 9-1-1 traffic.
- **Legacy Gateways:** Legacy Network Gateways (LNGs) are deployed at POIs to convert legacy OSP traffic to SIP, while LSRGs maintain transfer capabilities with neighboring legacy jurisdictions.

Additional Technologies & Interfaces

- **BCF:** SBCs and next-generation firewalls secure all ingress/egress points, normalizing SIP traffic and applying zero-trust security policies.
 - **Location & GIS Interfaces:** Secure connections to Location Information Servers (LIS) and the agency's authoritative GIS repositories continuously update the LVF and ECRF for accurate spatial routing.
 - **Downstream PSAP Interfaces:** Standardized NENA i3 interfaces ensure seamless, interoperable connections with CPE, CAD systems, and logging recorders for the delivery of multimedia and EIDO.
-

1.1.2 ESInet Interconnection

The ESInet must facilitate seamless interconnections with neighboring states or regions upon deployment. The ESInet shall use the Border Gateway Protocol (BGP) as the sole Exterior Gateway Protocol (EGP).

Motorola Response

Comply.

Newly established ESInets in cooperating states must be able to connect to the State ESInet within a designated timeframe. To ensure robustness and resilience:

- Interconnection should occur at a minimum of two mutually agreed-upon points to guarantee redundancy.

Motorola Response

Comply.

- Bandwidth provisioning must cater to **at least 200% of anticipated peak call volume**, ensuring ample capacity and robustness.

Motorola Response

Comply.

- Interconnecting methods and locations should be balanced equitably to manage costs effectively among partners.

Motorola Response

Comply.

- If neighboring ESInets do not adhere to the State's Differentiated Services Code Point (DSCP) specifications, the state's routers will remap DSCPs as deemed appropriate.

Motorola Response

Comply.

- The establishment of BGP between the State ESInet and neighboring networks is recommended.

Motorola Response

Comply.

All additional networks integrated with the ESInet must meet the specified minimum qualifications for interconnection to uphold security and performance standards. The State's security must be collaboratively protected by all involved network providers.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Seamless interconnections with neighboring states/regions upon deployment.

Motorola Response

Comply.

Our ESInet solution, designed for the Commission, is an open, standards-based "network of networks." Our solution natively supports NENA i3 v3 (STA-010.3f) Network-to-Network Interfaces (NNI), enabling seamless SIP-based call transfers and data exchange with neighboring states operating an ESInet immediately upon deployment. This ensures that a 911 call originating near a state border can be routed or transferred with its full PIDF-LO location and metadata intact. To support these capabilities, we have redundant interconnections to each neighboring ESInet.

- Connection capability for new ESInets within designated timeframe.

Motorola Response

Comply.

We offer connection capabilities for new ESInets through a scalable, standards-compliant architecture that facilitates quick onboarding and interoperability. Predefined interconnection criteria, documented procedures, and readily available configurations enable new partners to connect within the specified timeframe.

Collaboration with new ESInet partners commences early to synchronize technical, security, and routing requirements. This efficient approach reduces delays and guarantees timely, secure, and dependable interconnection. We are dedicated to finalizing these interconnections within the timeframe set by the Commission, supplying the necessary NNI specification documentation, and performing joint testing to ensure service continuity and routing precision.

- Minimum two interconnection points for redundancy. Bandwidth provisioning for 200% of peak call volume.

Motorola Response

Comply.

We will collaborate with adjacent ESInet providers to establish interconnections at two mutually agreed-upon locations that are geographically and physically diverse. Each site will possess independent connectivity, routing, and power to eliminate a single point of failure. Our strategy involves sizing and

provisioning ESInet bandwidth to a minimum of 200% of the anticipated peak call volume. Peak demand is determined by analyzing historical data, projected growth, and worst-case event scenarios.

- Equitable interconnecting methods/locations for cost management.

Motorola Response

Comply.

We will work together with the neighboring ESInet providers to establish interconnection points that strike a balance between technical performance and fiscal responsibility by leveraging existing carrier hotels and neutral exchange points.

- DSCP remapping if neighboring ESInets differ.

Motorola Response

Comply.

Our ESInet routers are configured to support ingress DSCP remapping, where applicable. In cases where a neighboring network employs a QoS framework that is not aligned with the requirements, our BCF will reassign tags to the incoming packets to correspond with the required traffic priority classifications (for instance, DSCP 46 for voice), thereby supporting uniform prioritization across the ESInet.

- Recommendation for BGP between networks.

Motorola Response

Comply.

Our proposed ESInet will use the BGP routing protocol between networks which allows for automatic dynamic path selection and rapid convergence.

- Minimum qualifications for additional integrated networks; and collaborative security protection by providers.

Motorola Response

Comply.

Providers that interconnect with the proposed Motorola ESInet must meet baseline security and compliance standards. This includes a documented security architecture, regular third-party risk assessments, TLS 1.3 encryption in transit and at rest, identity and access controls, PSAP

Credentialing Agency (PCA), logging and monitoring, incident response plans, and compliance with applicable laws and standards.

Providers should actively participate in shared security protection efforts. This includes timely threat and vulnerability sharing, coordinated incident response, joint security testing when required, adherence to common security policies, and clear communication channels for escalation and remediation.

1.2 External and PSAP Connectivity

1.2.1 Originating Service Provider (OSP) Connection

Contractors are responsible for facilitating all necessary connectivity to allow traffic to flow from OSPs into the ESInet.

- Upon acceptance, sufficient bandwidth must be provisioned to support OSP traffic irrespective of connection method (CAMA, SS7, IP, etc.).

Motorola Response

Comply.

- Points of Interconnection (POI) must be deployed with the greatest extent of diversity possible. This means that the contractor ***shall be required*** to identify any situations where OSPs lack diverse connections to the POI(s).

Motorola Response

Comply.

- Where diversity is limited from an OSP to the POI, and/or from the egress gateway to the PSAP, or restricted for any reason, **the contractor must identify this as a risk to their NG911 service and discuss options with the PSC for limiting or eliminating the exposure of an OSP or PSAP if a lack of diversity may cause a disruption.**

Motorola Response

Comply.

- Careful design should ensure **redundancy and diversity from the caller to the call-taker** to ensure that the system is as diverse and redundant as possible from end-to-end.

Motorola Response

Comply.

- Communications must enable smooth migration to the ESInet once operational, including aggregation of legacy 911 traffic into the core network.

Motorola Response

Comply.

- Contractors must continuously monitor the bandwidth at aggregation points to efficiently manage and increase bandwidth as required.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Facilitation of diverse and redundant connectivity for OSP traffic flow into the ESInet.

Motorola Response

Comply.

We will facilitate all necessary connectivity to ingest traffic from OSPs into Motorola's call routing service. All Points of Interconnection (POI) are geographically diverse, utilizing redundant building entrances to ensure no single point of failure. We collaborate with carriers to engineer diverse Meet-Me-Room (MMR) handoffs, providing a resilient ingress architecture.

- Provisioning of sufficient bandwidth for OSP traffic (CAMA, SS7, IP, etc.) upon acceptance.

Motorola Response

Comply.

We provision high-capacity ingress ports capable of handling the aggregate ingress OSP load. Our service natively supports legacy signaling (CAMA, SS7) via Legacy Network Gateways (LNG) and modern IP-based signaling (SIP/i3). We ensure that bandwidth is provisioned based on peak-busy-hour (PBH) calculations to prevent call queuing or signaling delays regardless of the connection method.

- Smooth migration to ESInet with aggregation of legacy traffic.

Motorola Response

Comply.

Our proven migration strategy ensures zero-downtime, by deploying redundant LNGs to convert legacy TDM/CAMA traffic into i3-compliant SIP/IP packets. This allows for the smooth transition of OSPs to the ESInet in phases aggregating all legacy traffic into the NGCS core.

- Redundant and diverse design for disruptions, interfacing with network gateways based on OSP capabilities.

Motorola Response

Comply.

Our proposed solution is designed to ensure continuity of operations during disruptions through a redundant and diverse architecture. We maintain a high degree of flexibility by interfacing with network gateways based on OSP capabilities.

Given that OSPs (including wireless, wireline, and VoIP carriers) function using a combination of modern and legacy technologies, our service accommodates the unique capabilities of each carrier.

- Identification of any risks to their system due to lack of diversity or redundancy from caller to call-taker.

Motorola Response

Comply.

Motorola conducts a comprehensive End-to-End Vulnerability Audit to identify any "single points of failure" within the call path. We recognize that true public-safety-grade resiliency requires not just redundancy (duplicated parts), but also geographic diversity (separate physical paths). Our risk identification process focuses on:

- **Originating Network Risks:** Identifying OSPs that utilize a single "aggregator" or selective router without a secondary failover path to the ESInet ingress.
 - **Transport Risks:** Detecting "common-trench" fiber routes where primary and secondary circuits share the same physical conduit, making them susceptible to a single backhoe cut.
 - **POI Risks:** Documenting instances where an OSP's handoff lacks diverse power or diverse entry points into the BCF.
 - **PSAP Egress Risks:** Assessing the "last mile" into the PSAP to ensure that the network edge infrastructure is served by at least two different carriers using non-overlapping physical paths.
-

- Identification of risks from limited diversity and options to mitigate exposure for OSPs or PSAPs.

Motorola Response

Comply.

We perform a comprehensive end-to-end vulnerability audit to identify and mitigate "single points of failure" between citizens and dispatchers. We minimize exposure to localized infrastructure outages by utilizing geographically diverse fiber entries, carrier-agnostic transport, and high-speed wireless broadband failover (LTE/5G/LEO). Each identified risk is proactively documented in the Project Risk Register with specific mitigation options, such as SD-WAN orchestration for sub-second failover, to ensure 99.999% operational availability.

- Continuous monitoring/increase of bandwidth at aggregation points.

Motorola Response

Comply.

Our NSOC continuously monitors traffic telemetry and health metrics across all ESInet aggregation points. Our system employs automated thresholds that generate capacity-planning alerts whenever bandwidth utilization reaches a predetermined level, typically 60% of provisioned capacity. This proactive approach ensures that we can scale bandwidth and increase port speeds ahead of demand.

1.2.2 PSAP Connection

At the point of system acceptance, the ESInet must guarantee sufficient bandwidth to support:

- **2 Mbps per PSAP + 2 Mbps per position** during standard operational conditions.
- **1 Mbps per PSAP + 1 Mbps per position** under conditions where network disruptions occur, which may include simultaneous failures of the largest link or comprehensive outages affecting all networks of a single ISP.

Motorola Response

Comply.

The contractor must commit to ongoing bandwidth monitoring throughout the contract duration and promptly increase capacity as necessary, including an annual growth factor of 10%.

Motorola Response

Comply.

The design must also facilitate interconnections with PSAP systems (like CAD and logging recorders), as well as with criminal justice networks and other secure public safety technologies, ensuring uninterrupted SIP traffic flow for 911 calls

Motorola Response

Comply.

The ESInet shall allow for all egress connectivity, including gateways, and be configured to establish the capability for traffic to flow from the ESInet into the PSAP.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Guaranteed bandwidth of 2 Mbps per PSAP + 2 Mbps per position under standard conditions and 1 Mbps per PSAP/position under disruptions (e.g., largest link failure or ISP outage).

Motorola Response

Comply.

We have provisioned the ESInet with a high-availability egress connection to the call handling system hosts that guarantees a minimum of 2 Mbps of dedicated bandwidth per PSAP, plus 2 Mbps for every call handling position during standard conditions. To ensure resiliency, our SD-WAN-orchestrated transport maintains a minimum bandwidth of 1 Mbps per site and 1 Mbps per position even during network disruptions, link failure or ISP outage.

Assumption: Per Customer Addendum #2 response to Pre-Bid Conference Question #8, Motorola assumes the current network provider is responsible for the provisioning and maintenance of the network connecting the call handling system host to the remote PSAPs.

- Commitment to ongoing bandwidth monitoring and increases with 10% annual growth factor.

Motorola Response

Comply.

Motorola commits to ongoing bandwidth monitoring and supporting an annual bandwidth growth factor of 10% for the duration of the contract. We utilize automated utilization thresholds to trigger capacity upgrades whenever sustained traffic exceeds 60% of provisioned bandwidth, ensuring the network remains ahead of demand.

Assumption: Per Customer Addendum #2 response to Pre-Bid Conference Question #8, Motorola assumes the current network provider is responsible for the provisioning, maintenance and growth of the network connecting the call handling system host to the remote PSAPs.

- Facilitation of interconnections with PSAP systems (CAD, logging recorders), criminal justice networks, and secure public safety technologies.

Motorola Response

Comply.

The ESInet is designed as a secure, interoperable gateway for PSAP technologies. We provide standardized interfaces to facilitate seamless integration with CAD systems, logging recorders, and Criminal Justice Information Services (CJIS) networks. Our service utilizes Service-Oriented Architecture (SOA) and NENA-compliant protocols to ensure that supplemental data from these systems can be securely transmitted across the ESInet.

- Ensuring uninterrupted SIP traffic for 911 calls.

Motorola Response

Comply.

The ESInet is designed as a secure, interoperable gateway for PSAP technologies. We provide standardized interfaces to facilitate seamless integration with CAD systems, logging recorders, and CJIS networks. Our service utilizes SOA and NENA-compliant protocols to ensure that supplemental data from these systems can be securely transmitted across the ESInet.

1.3 Legacy Interoperability

1.3.1 Legacy Network Gateway (LNG)

The Respondent must provide a Legacy Network Gateway (LNG) solution to serve as the ingress point for calls originating from legacy networks (e.g., wireline, wireless, VoIP) that have not yet transitioned to native i3 SIP origination. The LNG is responsible for converting legacy signaling to i3-compliant SIP and querying legacy ALI databases to obtain location information.

Motorola Response

Comply.

LNGs and/or LSRGs must conform to NENA-STA-010.3 and provide termination for all existing legacy OSPs until they migrate to i3 origination. The current solution utilizes an LSRG combining LNG and LSRG functions.

Motorola Response

Comply.

-
- Interface Compatibility:
 - The LNG must maintain interface compatibility with existing Selective Routers, allowing for minimal disruption and cost implications.

Motorola Response

Comply.

- Geographical Redundancy:
 - Legacy OSPs must have access to connections at two geographically diverse LNGs to enhance resilience.

Motorola Response

Comply.

- Legacy Support:
 - The LNG must be configured to manage legacy PSALI records, including migration processes outlined in the documentation provided.

Motorola Response

Comply.

LNG Connectivity to ESInet

The LNG must securely connect to the ESInet, receive calls from legacy network trunks (e.g., CAMA, MF), and interface with the ESInet's Border Control Function (BCF) to forward calls into the NG911 core.

Motorola Response

Comply.

Protocol Conversion (Legacy to SIP)

The LNG must convert legacy in-band signaling (e.g., CAMA wink-start, MF tones) and associated trunk supervision into i3-compliant SIP (RFC 3261) for processing by the ESInet.

Motorola Response

Comply.

ALI Query and Location Formatting

The LNG must use the Automatic Number Identification (ANI) received from the legacy call to perform a query against the appropriate legacy ALI database. It MUST then format the retrieved ALI data into a NENA-compliant Presence Information Data Format - Location Object (PIDF-LO) for inclusion in the outbound SIP INVITE.

Motorola Response

Comply.

Security, Logging, Monitoring, and Redundancy

The LNG, as a critical ESInet functional element, must adhere to the same stringent requirements for security, logging, monitoring, and redundancy as other core components to ensure system integrity and high availability.

Motorola Response

Comply.

If separate LNGs are proposed, they must:

- Maintain interfaces similar to current systems
- Support TTY to RTT conversion
- Provide E2 connections to all MLCs, GMLCs, and VPCs
- Be positioned outside the ESInet, before the BCF
- Support ElementState and ServiceState functionality

Motorola Response

Comply.

Each component has specific requirements for capacity, performance, integration, and conformance with NENA standards.

Motorola Response

Comply.

The solution must maintain appropriate spare parts at various locations to ensure immediate system restoration when needed, with specific requirements for inventory management, replacement schedules, and on-site spares at data centers.

Motorola Response

Comply.

The LNG must support the Service Order Activation (SOA) interface towards the legacy OSP, store data in the Location Database in LVF-valid form and convert to and from the legacy data format using the MCS.

Motorola Response

Comply.

The LNG shall support:

- Error checking
- GIS-based MSAG (for legacy OSP use)
- The Service Order Activation (SOA) interface towards the legacy OSP, store data in the Location Database in LVF-valid form and convert to and from the legacy data format using the MCS
- Service Order Address Validation
- Service Order Error checking
- Service Order history available/viewable for every telephone number
- Coordination with Telecommunications providers:
 - OSPs will be able to manage/make updates to their records directly in the database without having to submit SOI
 - OSPs will be able to run performance/statistical reports on their No Record Found (NRF)/Discrepancy and SOI processing
 - OSPs will be able to view discrepancies and NRFs directly from the web interface real time
- Data import / export
- Data integrity and availability
- ALI updates
 - OSP's have the ability to manually update their own records
 - OSP's have the ability to lock and unlock their own records
 - All manual updates be tracked in history
- Customer access to data
- Telco access to data

- Bulk modifications
- PSALI functionality
- Database reports
- NRF process
 - ALI discrepancies
- Tracking, reporting and timestamp for discrepancies and NRFs.
- Service Order exceptions
- ALI database audit
- MSAG database audit

Motorola Response

Comply.

The State expects the LNG to maintain connections to Text Control Centers (TCCs) so that NG PSAPs maintain a complete standard (NENA-STA-010.3) connection for Short Message Service (SMS) calls to 911 from legacy OSPs via the LNG.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LNG conformance to NENA-STA-010.3 for legacy OSPs until i3 migration.

Motorola Response

Comply.

We adhere to NENA-STA-010.3f by utilizing LNGs to facilitate legacy OSP interconnection throughout the transition to i3.

- Interface compatibility with existing Selective Routers.

Motorola Response

Comply.

Our proposed solution ensures seamless transition through our LSRG, which provides standardized NENA-compliant interfaces to bridge existing Selective Routers with the NGCS call routing service.

This architecture enables bidirectional call and data transfers, allowing calls to be routed between legacy and NG9-1-1 networks while preserving vital metadata and signaling.

- Geographically diverse connections for legacy OSPs.

Motorola Response

Comply.

Our solution provides geographic diversity for legacy OSPs by deploying redundant LNGs across physically separate POI locations. This architecture ensures that legacy trunks, including CAMA, SS7, and TDM, have active, simultaneous connections to multiple ingress points, preventing any single-site failure from disrupting call delivery to the ESInet.

- Management of legacy PSALI records with migration processes.

Motorola Response

Comply.

We manage the migration of legacy PSALI records by systematically ingesting existing NENA 2.x data formats into our LDB. During this transition, we perform automated validation of legacy records against the provided GIS data to ensure that "tabular" addresses are accurately converted into precise "geospatial" coordinates. This process allows enterprise and Multi-Line Telephone System (MLTS) data to remain operational throughout the cutover, ensuring that precise floor and room-level location information is preserved as calls move from legacy trunks to the ESInet.

- TTY to RTT conversion.

Motorola Response

Comply.

Our LNG provides TTY to RTT conversion, allowing legacy TTY devices to communicate with PSAPs supporting RTT. Our gateway performs transcoding of character-by-character Baudot tones into RFC 4103-compliant IP packets, supporting two-way emergency conversations.

- E2 connections to MLCs/GMLCs/VPCs. Positioning outside ESInet before BCF.

Motorola Response

Comply.

Our proposed LNG provides E2 interfaces (as defined in J-STD-036) to establish secure, real-time connections with MLCs, GMLCs, and VPCs. These connections allow the gateway to perform location queries for wireless and nomadic VoIP calls, ensuring that Phase 1 and Phase 2 location data is retrieved and attached to the emergency call before it enters the ESInet. By maintaining these critical data links, the LNG ensures that location-based routing remains accurate for all non-native i3 callers, fulfilling the NENA i3 requirement for location interworking across all OSPs.

- ElementState/ServiceState support.

Motorola Response

Comply.

Our proposed LNG supports ElementState and ServiceState functionality as defined in NENA-STA-010.3, enabling real-time observability into the gateway's operational health. Through a standardized SUBSCRIBE/NOTIFY mechanism using RESTful APIs and JSON payloads, the gateway provides the Motorola NSOC with automated updates on the availability of its internal FEs and the status of its outward-facing emergency services.

1.3.2 Legacy Selective Router Gateway (LSRG)

A Legacy Selective Router Gateway (LSRG) must serve as the interface for legacy selective routers to terminate ISUP SS7 trunks utilizing an inter-tandem trunk group method of termination.

Motorola Response

Comply.

The LSRG must convert the call signaling to SIP/RTP, query the existing ALI data management system to retrieve location information for the call and then route the call to the next nominal "hop" based on a LoST query to an ECRF.

Motorola Response

Comply.

Additionally, the LSRG must be able to facilitate bi-directional communications with the legacy selective routers for both voice and data (star codes) transactions.

Motorola Response

Comply.

If Respondents utilize an LSRG for their proposed solution, they must include a timeline and plan for removing the LSRG during the contract period. The LSRG is to be only a temporary solution that can be used to initially gateway OSP traffic.

Motorola Response

Comply.

Any LSRG implemented as part of the Contractor's solution must conform to the NENA Legacy Selective Router Gateway (LSRG) Standard (NENA-STA-034.1-2022), and should be deployed to align with the relevant sections of the NENA NG9-1-1 Transition Plan Considerations Information Document (NENA-INF-008.2-2013).

Motorola Response

Comply.

LSRG Connectivity to ESInet and Legacy SR

The LSRG must provide a secure interface to the ESInet to receive routing queries from the ECRF and a separate, secure interface compatible with the legacy Selective Router's query/response protocol.

Motorola Response

Comply.

Routing Protocol Conversion (LoST to Legacy)

The core function of the LSRG is to receive a standards-based Location-to-Service Translation (LoST) protocol query (RFC 5222) from the ECRF, translate it into a format the legacy SR can process (often a proprietary format or a simplified query containing an ESN), and translate the SR's response back into a LoST response for the ECRF.

Motorola Response

Comply.

Security, Logging, Monitoring, and Redundancy

The LSRG must meet the same core requirements for security, logging, monitoring, and geodiverse redundancy as other critical ESInet FEs to ensure the integrity and availability of call routing.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Interface for legacy Selective Routers via ISUP SS7 trunks.

Motorola Response

Comply.

Our proposed solution provides a high-availability LSRG that acts as a "tandem" interface to existing legacy Selective Routers. The gateway supports standard ISUP SS7 trunks, allowing the ESInet to appear as a standard peer switch to the legacy network. This ensures that calls can be routed or transferred between the legacy TDM environment and the NGCS call routing service without requiring any hardware modifications to the existing SR infrastructure.

- Conversion to SIP/RTP.

Motorola Response

Comply.

Our LSRG performs real-time media and signaling transcoding, converting legacy ISUP/SS7 signaling into i3-compliant SIP (RFC 3261) and analog/TDM audio into RTP/IP streams. This normalization allows legacy calls to be processed by the ESRP and delivered to PSAP call handling systems.

- ALI query and LoST-based routing.

Motorola Response

Comply.

Upon receiving a transferred legacy call, our LSRG initiates an ALI query to retrieve location data. It then reformats this data into a PIDF-LO and performs a LoST query to the ECRF to determine the appropriate next-hop PSAP. This ensures that even calls originating from legacy routers are routed using the State's authoritative GIS-based routing rules.

- Bi-directional communications for voice/data (star codes).

Motorola Response

Comply.

Our LSRG supports full bi-directional communication, enabling both voice and signaling data (star codes) to pass between the legacy and NG9-1-1 networks. This preserves existing operational workflows for dispatchers, ensuring that legacy features remain functional while they are bridged into the ESInet.

- Timeline/plan for LSRG removal as temporary solution for OSP traffic.

Motorola Response

Comply.

We view the LSRG as a transitional bridge rather than a permanent fixture. The preliminary project schedule includes a phased approach to decommission the use of LSRGs to interface with existing legacy selective routers that aligns with the OSP migration to the NGCS call routing service. Based on the preliminary project schedule, we anticipate decommissioning the LSRGs by August 2028.

- Deployed LSRG (where applicable) in conformance with NENA LSRG Standard (STA-034.1)

Motorola Response

Comply.

Our proposed LSRG is designed and deployed in conformance with NENA-STA-034.1. This ensures the LSRG adheres to standardized interworking protocols for both legacy-to-i3 and i3-to-legacy call flows, facilitating interoperability as required for the State's transition.

1.3.3 Legacy PSAP Gateway (LPG)

The State requires Legacy PSAP Gateways (LPGs) that conform to NENA-STA-010.3. LPGs shall provide origination for all legacy PSAPs until those PSAPs migrate to i3 termination. LPGs must allow PSAPs to continue to use existing equipment and processes except where NENA-STA-010.3 requires change (for example, use of Pseudo-Automatic Number Identification [pANI]). Each LPG shall connect legacy PSAPs to the ESInet using SIP and legacy interfaces such as CAMA and ALI and shall convert NG911 SIP signaling and media to legacy protocols such as TDM and ISDN to maintain compatibility.

Motorola Response

Comply.

Protocol Conversion (SIP to Legacy)

The LPG must convert the SIP-based signaling and media from the ESInet into legacy circuit-switched formats (e.g., CAMA, ISDN PRI) that are compatible with the legacy PSAP's CHE.

Motorola Response

Comply.

Location and ALI Integration

The LPG must extract location information (PIDF-LO) from the incoming SIP signaling and convert it into a legacy Automatic Location Identification (ALI) format for delivery to the PSAP's ALI database/controller.

Motorola Response

Comply.

Text Support (TTY to RTT Conversion)

The LPG must support interworking between Real-time Text (RTT) on the ESInet, and legacy Baudot-based Teletypewriter (TTY) devices used in the PSAP, ensuring seamless communication for hearing-impaired users.

Motorola Response

Comply.

Call Transfer Support

The LPG must support call transfer scenarios, including the ability to relay transfer requests from the legacy PSAP back into the ESInet to enable transfers to other NG911-capable agencies or PSAPs.

Motorola Response

Comply.

Logging and Reporting

The LPG must generate detailed logs for all call processing events, alarms, and system activities and forward them to a central logging service in a standard format (e.g., Syslog) as defined by NENA standards.

Motorola Response

Comply.

Security Mechanisms

Technical Requirements



The LPG must implement robust security measures, including access control, authentication, and encryption, to protect the interface between the ESInet and the legacy PSAP network, adhering to NG911 security standards.

Motorola Response

Comply.

Monitoring and Maintenance

The LPG must be capable of being monitored for operational status, performance, and alarms. It must support standard monitoring protocols (e.g., SNMP) and provide mechanisms for remote administration and maintenance.

Motorola Response

Comply.

Geo-Diversity and Redundancy

The LPG must be deployed in a geographically diverse and redundant configuration to ensure high availability and failover capabilities, preventing a single point of failure from isolating a legacy PSAP.

Motorola Response

Comply.

Discrepancy Reporting

The LPG must support a mechanism for reporting discrepancies, such as call routing errors or ALI data problems, from the legacy PSAP environment back to the NG911 systems Discrepancy Report service.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- The LPG must be able to maintain the PSAP's existing ALI format.

Motorola Response

Comply.

Our LPG is engineered to translate modern PIDF-LO (geospatial) location data back into the legacy tabular ALI formats (e.g., NENA 2.1) currently expected by the PSAP's call-handling equipment. The gateway queries its internal LDB or external legacy ALI hosts to ensure that when a call is delivered via traditional MF or Enhanced MF (E-MF) trunks.

- The LPG must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3.

Motorola Response

Comply.

In full compliance with NENA-STA-010.3f, our LPG supports the SUBSCRIBE/NOTIFY framework for both ElementState (internal component health) and ServiceState (end-to-end service availability). This allows the State to subscribe to real-time status updates and receive standard state-change notifications.

- The State must be able to subscribe to ServiceState and receive the standard state change

Motorola Response

Comply.

The LPG supports the NENA i3v3 (STA-010.3f) event framework, which utilizes a REST/JSON-based SUBSCRIBE/NOTIFY mechanism for monitoring. The State will have the ability to subscribe to the LPG's ServiceState, allowing it to receive standardized notifications whenever a ServiceState change occurs.

- LPG connections shall allow for PSAPs to directly connect systems (cable IP) to the ESInet

Motorola Response

Comply.

The LPG acts as the secure physical and logical handoff point between the ESInet and the legacy PSAP's local infrastructure. We provide the necessary connections to facilitate the interface from the existing legacy call handling system directly to the ESInet. This design ensures that even though the internal PSAP systems are legacy, their connectivity to the ESInet is managed through the LPG.

- LPG queries ALI databases and maps NG911 location data to legacy formats.

Motorola Response

Comply.

To ensure dispatchers see familiar data, our LPG performs "reverse interworking" by taking the PIDF-LO (geospatial) location object from an i3 call and mapping it back to traditional tabular ALI formats (e.g., NENA 2.x). The LPG queries either a legacy ALI database or the NG9-1-1 LDB to retrieve the specific civic address or coordinates, then formats this data into the precise character-delimited string expected by the legacy PSAP's equipment.

- Converts TTY to RTT for text-to-911 in legacy PSAPs.

Motorola Response

Comply.

For PSAPs that have not yet upgraded to native IP-based text handling, the LPG includes a built-in transcoding function that converts RTT characters into legacy Baudot TTY tones. This enables a citizen using a modern smartphone to communicate via text with a dispatcher who is still using a legacy TTY/TDD machine. The LPG ensures this conversion is bidirectional and synchronous, maintaining the conversational flow required for emergency assessment.

- Supports call transfers to/from legacy PSAPs, mapping i3 transfers to legacy systems.

Motorola Response

Comply.

Our LPG supports inter-PSAP transfers by translating i3 SIP-based transfer signals into the legacy signaling (e.g., 10-digit or E-MF signaling) used by legacy PSAPs. When an i3 PSAP transfers a call to a legacy PSAP, the LPG ensures the voice path is maintained and that the associated location data is provided to the receiving agency which matches their existing ALI format.

- Logs call events, protocol conversions, and errors; supports discrepancy reporting.

Motorola Response

Comply.

The LPG maintains time-stamped logs of all system activities, including every protocol conversion and signaling event. These logs are stored in a NENA-compliant i3 log format, which allows tracking of a call from ingress to the final delivery at the PSAP call handling system.

- Implements TLS and authentication for secure connectivity.

Motorola Response

Comply.

The LPG supports the use of TLS for all IP-based communication. The use of TLS allows for encryption and security connectivity across the ESInet.

- Monitors LPG performance; supports maintenance with minimal disruption.

Motorola Response

Comply.

We utilize automated health probes and SNMP-based monitoring to track LPG performance metrics such as CPU load, memory utilization, and port availability. Our maintenance procedures leverage the gateway's high-availability design, allowing for "rolling" software updates where traffic is shifted to a secondary node while the primary is serviced. This ensures that routine maintenance or emergency patches can be applied without causing any downtime or dropped calls at the PSAP.

- LPG deployed with geo-redundancy to ensure high availability.

Motorola Response

Comply

To eliminate single points of failure, we will deploy the LPG in a redundant and geo-diverse architecture. For a single host call handling system with remote, redundant LPGs would be deployed at the single host site.

- Reports errors in call delivery, location, or protocol conversion.

Motorola Response

Comply.

The LPG supports error-detection logic that triggers immediate alerts if it encounters a failure in call delivery, malformed location data, or a protocol mismatch. These errors are reported in real-time to the Motorola NSOC and recorded in the system logs for post-incident analysis.

1.4 Network Behavior and Performance

1.4.1 ESInet IP Routing

The ESInet must follow the NENA standards to ensure that IP routing across the ESInet can handle all traffic effectively under varying conditions. Ongoing bandwidth assessments, risk assessments, diversity, and redundancy testing must be documented and updated in a configuration management database as the ESInet evolves. Proactive measures to trace IP routing within the diverse and

redundant paths is required. Any change to the system must include testing of IP routing failover mechanisms prior to acceptance of a change.

Motorola Response

Comply.

No specific link shall be provisioned with **more than 50% of the physical limit** of that link to allow for expansion without physical changes to the link, router, or switch to which it connects. As changes in the network are completed, the IP address plan shall be updated and remain accessible to the State or designee.

Motorola Response

Comply.

- Every element proposed supports both IPv4 and IPv6 (dual stack).

Motorola Response

Comply.

- All elements in the network have globally routable IP IPv4 and IPv6 addresses.

Motorola Response

Comply.

- The network shall use one Interior Gateway Protocol (IGP) throughout, and no routers use Routing Information Protocol (RIP).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance with NENA standards for handling traffic under varying conditions.

Motorola Response

Comply.

Our proposed ESInet architecture adheres to NENA-STA-010.3f (i3v3) and NENA-STA-019.2 for call processing metrics. The QoS strategy utilizes DSCP marking to prioritize 9-1-1 SIP signaling (DSCP 40) and RTP media (DSCP 46) above all other data. This ensures that during a network congestion event, such as regional weather disasters where call volumes exceed 150% of peak, maintaining packet loss below 0.5%, jitter under 15 milliseconds, and (one-way) latency below 25 milliseconds is our priority.

- Documentation of ongoing bandwidth assessments, risk assessments, diversity and redundancy testing in a configuration management database.

Motorola Response

Comply.

We maintain a centralized repository to document the ESInet **configuration**, **maintenance** activities, and **assessments**. Our documentation process tracks every circuit, node, and functional element, specifically storing **Diversity Audits** that map physical network paths.

- Proactive measures to trace IP routing in diverse and redundant paths.

Motorola Response

Comply.

We employ proactive network telemetry and traffic probes to continuously trace and visualize IP routing paths across the ESInet. These traffic testing tools simulate 9-1-1 call flows to detect route changes or latency spikes. If a primary path's performance degrades, our Bidirectional Forwarding Detection (BFD) triggers a sub-second BGP reroute to a diverse secondary path, with the event automatically logged as a performance alert in the NSOC.

- Testing of IP routing failover mechanisms prior to any system change acceptance.

Motorola Response

Comply.

We adhere to a rigorous change management policy where no update, hardware, or software is accepted without successful failover testing. Before a "Change Window" is closed, technicians will execute a live failover test (e.g., disabling a primary BCF or Core Router) to verify that traffic re-converges in less than 54 milliseconds. Results of these pre-acceptance tests, including rollback procedures and performance captures, are attached to the Change Request and archived in the CMDB for the Commission's review.

1.4.2 ESInet Bandwidth

The ESInet is expected to deliver sufficient end-to-end bandwidth to accommodate traffic to and from PSAPs effectively.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Adequate sizing must consider 911 voice and video calls, text communications, data transmissions, and a calculated surge factor based upon the State of Nebraska PSAPs.

Motorola Response

Comply.

The ESInet bandwidth calculation includes the aggregate traffic overhead associated with concurrent voice, Real-Time Text (RTT), and emerging multimedia/video streams as defined in this RFP. Our ESInet sizing calculations incorporate a surge factor based on the RFP requirements to ensure the network remains non-blocking during mass-calling events or regional disasters. Additionally, if a surge in 9-1-1 calls occurs, the underlying IP transport provides the necessary headroom to prevent packet loss or latency-induced audio jitter.

- An **annual growth factor of 10%** must be incorporated into capacity planning.

Motorola Response

Comply.

The ESInet bandwidth estimates incorporate built-in growth capability to accommodate a 10% annual growth factor over the term of the contract.

- Bandwidth sharing with other networks within the State of Nebraska is encouraged, **especially for secondary routes, provided the contractor implements provisions to ensure that using these networks does not impact the primary ESInet performance.**

Motorola Response

Comply.

To protect primary ESInet performance, we implement SD-WAN orchestration and strict Logical Partitioning (VLAN/VRF). These provisions ensure that 9-1-1 traffic is isolated in a "High Priority" queue; if a shared network experiences congestion from non-emergency traffic, our QoS policies automatically preempt other data to guarantee 9-1-1 call delivery with zero impact on performance.

- The ESInet should be structured for future expansion, allowing scalable growth throughout the duration of the contract without impeding current services. A detailed plan should outline how the ESInet will readily accommodate increases in bandwidth, as necessary.

Motorola Response

Comply.

Motorola's ESInet architecture is structured to seamlessly accommodate future expansion and scalable growth throughout the life of the contract, ensuring that capacity upgrades never impede current mission-critical services. The following plan outlines how our network will readily adapt to necessary bandwidth increases as your operational needs evolve:

- **Oversized Network Design:** Each network link, along with core network components such as firewalls and routers, is intentionally oversized to account for a 20% growth margin upon initial deployment.
 - **50% Growth Capacity:** The service is fully scalable to support voice and data traffic growth of up to 50 percent without requiring the replacement of any critical hardware or software components.
 - **Peak Volume Handling:** The ESInet design is capable of maintaining the bandwidth necessary to support 150% of peak call volumes to ensure performance is not adversely affected during high-traffic events.
 - **Incremental Expansion:** Because the service utilizes a modular architecture, expansion of the technology stack is incremental with no known limits to upward expansion, meaning no "forklift" updates are required to scale the transport networks for additional traffic.
 - **Immediate Availability:** If sudden growth occurs due to PSAP consolidation or the addition of new workstations, sufficient bandwidth is already allocated to handle the immediate demand until the circuits can be formally re-configured for the permanent capacity increase.
 - **Automated Threshold Management:** The NSOC proactively monitors the ESInet to prevent bottlenecks. If any network path sustains 60% utilization over 24 hours, the system automatically triggers a bandwidth increase. This allows the ESInet to proactively scale to meet the 10% annual growth requirement defined in the RFP before network congestion can occur.
-

- A detailed plan for scalable expansion throughout the contract without impeding services.

Motorola Response

Comply.

Our Bandwidth Expansion Plan follows a multi-tiered approach to ensure that capacity always precedes demand:

- **Logical Provisioning (Hitless Upgrades):** We provision PSAP and Core circuits with "Elastic" bandwidth. While an agency, for example, may initially subscribe to 10 Mbps, we provision a physical 20 Mbps. This allows us to increase the logical bandwidth limit remotely via our NOC without any physical technician visit or service interruption.
 - **Proactive Threshold Management:** We implement automated Utilization Alerts. When any circuit sustains 60% utilization over 24 hours, a capacity-planning ticket is generated to trigger a bandwidth increase, ensuring the mandated 10% annual growth is exceeded if actual usage trends higher.
 - **Modular Core Scaling:** Our VESTA NXT Router logic is distributed across multiple geo-redundant nodes. As PSAP call volume or data payload increases (e.g., widespread 9-1-1 video adoption), we can scale the core horizontally by adding virtualized instances, ensuring zero impact on active call-taking services.
-

1.4.3 Quality of Service (QoS)

The ESInet must provide Quality of Service (QoS) features at all ingress, core, and egress points.

Motorola Response

Comply.

The ESInet must employ DiffServ throughout, adhering to packet marking specifications per NENA-STA-010.3. A commitment to maintaining packet loss below 0.5%, jitter under 15 milliseconds, and (one-way) latency below 25 milliseconds is required during standard operational periods.

Motorola Response

Comply.

- Performance metrics for these characteristics should be established on a standby measurement basis, with the State stakeholders allowed to initiate specific measurements as required.

Motorola Response

Comply.

- Regular reporting must provide comprehensive insights into network performance metrics, including averages and worst-case scenarios.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Employment of DiffServ throughout with packet marking per NENA-STA-010.3.

Motorola Response

Comply.

We employ Differentiated Services (DiffServ) at every ingress, core, and egress node of the ESInet. We strictly adhere to the packet marking specifications defined in NENA-STA-010.3f, utilizing DSCP 46 (Expedited Forwarding) for all emergency voice and Real-Time Text (RTT) media to ensure immediate, low-latency delivery. Signaling traffic is marked with DSCP 40 (CS5) or DSCP 34 (AF41) to prioritize call setup and routing instructions, ensuring that mission-critical signaling is never queued behind non-emergency data.

-
- Commitment to packet loss below 0.5%, jitter under 15 milliseconds, and one-way latency below 25 milliseconds during operations.

Motorola Response

Comply.

We commit to following the performance benchmarks for all 9-1-1 traffic across the ESInet.

- **Packet Loss:** less than 0.5% (To prevent audio clipping and signaling failure).
- **Jitter:** less than 15 ms (To ensure high-fidelity voice and text synchronization).
- **One-Way Latency:** less than 25 ms (To provide instantaneous communication between caller and call-taker).

These targets are enforced through strict bandwidth policing and QoS queuing at all network boundaries.

-
- Standby measurement basis for performance metrics with State-initiated measurements.

Motorola Response

Comply.

Our ESInet monitoring architecture uses active probes to continuously verify network health and performance without impacting live traffic. We will work with the State regarding a standby measurement basis for performance metrics with State-initiated measurements.

-
- Regular reporting on network performance including averages and worst-case scenarios.

Motorola Response

Comply.

We provide comprehensive Network Performance Reports on a monthly basis, or as requested by the State. These reports detail:

- MoS score, average latency, jitter, and % packet loss.
 - Identification of performances during peak-busy-hour (PBH) surges.
 - Proactive identification of circuits nearing utilization thresholds to facilitate the 10% annual growth planning.
-

1.4.4 Traffic Flow Requirements

Respondents must describe how traffic will flow from end to end across the network in a fashion that is compliant with applicable standards. ESInet and NG Core Services functions be described to allow the evaluator to clearly identify where specific operations on the traffic occur. If necessary, diagrams may be used to assist the visualization of traffic flow through the proposed solution.

Motorola Response

Comply.

The ESInet and NGCS must operate in concert with one another to establish the flow of traffic from the caller to the call-taker. This flow of traffic utilizes physical and logical connections to the resources required for call delivery. Traffic flow shall include a description of traffic flow under **NORMAL** operating conditions and traffic flow under **ABNORMAL** operating conditions.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- End-to-end traffic flow description compliant with standards.

Motorola Response

Comply.

When a call enters the network, it undergoes a series of standardized operations to ensure security, accuracy, and reliability which aligns with the NENA i3 standards.

- **Security Screening (BCF):** The BCF acts as the first line of defense, performing firewalling and session border control to sanitize SIP signaling and protect against cyber threats.

- **Routing Orchestration (ESRP):** The ESRP receives the call and queries the ECRF to find the correct destination. It also manages queuing and applies policy rules.
 - **Geospatial Routing (ECRF):** The ECRF uses the caller's latitude/longitude (PIDF-LO) and compares it against the authoritative GIS database to return the URI of the target PSAP.
 - **Policy Application (PRF):** The PRF checks the target PSAP's state. If the PSAP is logged off or in an "overflow" state, the PRF redirects the call to a pre-defined backup based on the agency's business rules.
-

- Identification of operations on traffic in ESInet and NGCS.

Motorola Response

Comply.

Operations on traffic within the ESInet and NGCS follow a rigorous sequential process designed to validate, route, and secure every emergency request. Traffic first encounters the BCF, which performs deep packet inspection and signaling "sanitization" to ensure all incoming SIP traffic is authenticated and free of malicious intent. Once secured, the ESRP orchestrates the call by querying the ECRF to determine the correct destination based on real-time GIS data, while simultaneously applying PRF rules to account for PSAP availability or overflow conditions.

- Diagrams for visualization if necessary; traffic flow under normal and abnormal conditions.

Motorola Response

Comply.

The system is designed to maintain traffic flow continuity during normal and abnormal conditions:

Normal Conditions: Traffic flows through a primary gateway, being routed geospatially by the ECRF, and being delivered directly to the primary PSAP's call-handling equipment.

Abnormal Conditions (Failover): If a network path is severed, BGP triggers a sub-second reroute to a diverse physical path. If a PSAP becomes unreachable, the ESRP automatically invokes Call Diversion policies via the PRF to route calls to an alternate PSAP based on customer-defined policy routing rules (PRR), ensuring no call is dropped.

- Handling of use cases such as legacy OSP to NG PSAP, NG OSP to NG PSAP, Internet to NG PSAP, text/ALI/GIS traffic, virtual PSAPs, BCF to ECRF, ECRF to SI/ESRP/PSAP/LPG, LSRG to OSP, OSP to LNG, logging/recording, and monitoring/management. Additional or modified use cases specific to the solution should be expanded upon.

Motorola Response

Comply

As specified in the RFP, Section 10.1 covers the various use cases listed in this requirement. For detailed responses, please refer to Section 10.1.

1.4.5 Traffic Shaping

Respondents must include a description of where traffic shaping will be employed, detailing the techniques used and their intended benefits. A formal **traffic shaping policy document** must be created, ensuring transparency and regular updates are made available to State personnel.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Description of where traffic shaping is employed, the techniques used, and their intended benefits.

Motorola Response

Comply.

Where Traffic Shaping is Employed: Traffic shaping and QoS are comprehensively implemented across the entire Motorola ESInet. Specifically, within the scope of the RFP, these features are deployed on the PSAP-facing network (PSAP ESInet), which utilizes a modern SD-WAN architecture. The traffic shaping is enforced end-to-end and seamlessly extends beyond the ESInet boundaries when interconnecting with third-party networks or service providers to ensure consistent end-to-end performance.

Techniques Used: Motorola relies on a capacity-first design that utilizes deliberate capacity engineering and continuous utilization monitoring to keep the network well below saturation thresholds. To manage traffic shaping and QoS, the architecture employs the following techniques:

- **Application-Aware Classification and Marking:** Traffic is identified via protocol inspection and application recognition, then marked using standardized DSCP values aligned with NENA guidelines.
- **Service Class Mapping:** Traffic is sorted into specific priority tiers: Real-Time (highest priority for RTP/RTCP voice media), Transactional (high/medium priority for SIP signaling and WebRTC), and Bulk/Best Effort (deprioritized during congestion).
- **Weighted Queuing and Scheduling:** Real-time traffic is given a significantly higher scheduling weight (e.g., 70%) to ensure latency-sensitive flows are handled first. The system uses dynamic bandwidth sharing rather than strict policing to avoid introducing packet loss.
- **Dynamic Multipath Optimization (DMPO):** The SD-WAN fabric operates in a true multipath mode with continuous monitoring of latency, jitter, packet loss, and bandwidth. DMPO actively improves packet delivery using:
 - **Per-Packet Steering:** Distributes traffic packet-by-packet across the best available paths.

- **Forward Error Correction (FEC):** Recovers packet loss on lossy circuits without needing retransmission.
- **Packet Duplication:** Replicates critical packets across multiple paths to ensure delivery during transient loss.
- **Adaptive Jitter Buffering:** Dynamically compensates for delay variation to maintain audio quality.
- **Sub-Second Seamless Failover:** Instantly redirects traffic upon link degradation or failure.
- **Quality of Experience (QoE) Thresholds:** Continuously evaluates link health and automatically triggers path changes if performance degrades to ensure application performance stays within acceptable bounds.

Intended Benefits: The primary benefit of this traffic shaping strategy is to ensure deterministic application performance under all network conditions, guaranteeing that mission-critical NG9-1-1 services (Call Traffic, Signaling, and Critical Applications) operate without degradation even during transient congestion or microbursts. Additional benefits include:

- Deterministic prioritization of NG9-1-1 voice and signaling, ensuring call clarity and reliability.
 - Minimized latency, jitter, and packet loss for real-time emergency communications.
 - Efficient and maximized bandwidth utilization by steering critical traffic to the highest-quality links while allowing lower-priority traffic to use alternate circuits.
 - Seamless failover with absolutely no session interruption during circuit degradation.
 - Consistent, end-to-end QoS enforcement that strongly aligns with public safety and NENA best practices.
-
- Creation of a formal traffic shaping policy document with transparency, regular updates, and availability to State personnel.

Motorola Response

Comply.

We rely on a rigorous standards-based QoS framework which is governed by detailed internal engineering guidelines. These guidelines clearly define the classification, marking, queuing, and traffic handling behaviors across all of their ESInet domains.

To ensure full transparency, regular updates, and availability to State personnel, we propose direct collaboration. Our ESInet Network Architects and QoS/Traffic Shaping subject matter experts are available to engage directly with State personnel. Through this collaboration, they will provide additional details on our approach to ensure the State has a clear, transparent understanding of the ESInet traffic shaping strategy and associated documentation.

1.4.6 ESInet Network Time

Network Time Protocol servers must be provided. The NTP servers must provide service to all elements in the ESInet including all PSAPs and other agencies on the ESInet. Time service must permit every system and every agency to maintain time within 1 millisecond of absolute time with 4

nines (99.99%) availability. The network shall have a hardware clock. However, in no circumstances, including failure of the hardware clock, must time as maintained by the time server(s) vary by more than 20 milliseconds from absolute time.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Provision of NTP servers serving all ESInet elements (NGCS FEs, PSAPs, agencies) within 1 millisecond of absolute time with 4 nines (99.99%) availability.

Motorola Response

Comply.

Our solution provides dedicated, high-precision NTP servers to all ESInet FEs, ensuring that all network timestamps remain within 1 millisecond of absolute Coordinated Universal Time (UTC). We support 99.99% availability (four nines) for the timing service through a distributed, hierarchical architecture. Stratum 1 master clocks at each core site act as the primary reference, synchronized to UTC via GNSS/GPS.

To mitigate risks while meeting NENA's strict accuracy requirements, PSAPs should implement an **internal** Stratum 1 Master Clock (often referred to as a NetClock). The Master Clock acts as the authoritative NTP server for the entire internal PSAP network. This eliminates the need to open Port 123 to the outside internet, protecting the network from external NTP-based attacks while ensuring every device in the PSAP is perfectly synchronized. NTP operates over UDP on Port 123. To pull time from an external internet source, the PSAP must leave Port 123 continuously open on its external firewall. This creates a known, universally targeted hole that hackers can exploit to gain access to the internal network.

- Preference for hardware clock but ensuring no more than 20 millisecond variances even on failure.

Motorola Response

Comply.

In alignment with State preferences, our approach employs dedicated hardware-based Stratum 1 clocks (such as GPS-disciplined oscillators) at each core node instead of depending on software or virtualized time sources. Should a primary clock fail, the system seamlessly shifts to a peer reference or its internal holdover source, maintaining the time variance remains within 20 milliseconds of absolute UTC, even in the most challenging failure situations.

- Descriptions of NTP service provision, confirmation of 1 millisecond accuracy with 4 nines availability, and meeting 20 millisecond variance threshold.

Motorola Response

Comply.

We confirm that our NTP service provision meets all requested benchmarks: 1ms accuracy, 99.99% uptime, and a maximum 20ms variance during holdover. To describe the service description, we provide the following:

- **NOC Telemetry:** 24/7 monitoring of Stratum levels and time-offset metrics for all ESInet elements.
 - **Audit Logs:** Millisecond-accurate event logging at the i3 Logging Service, traceable to our Stratum 1 reference.
 - **Failover Validation:** Documentation of automated "sanity checks" where the system rejects malfunctioning clocks to prevent time-drift propagation.
-

1.5 Resilience and Service Levels

1.5.1 ESInet Availability

The ESInet must maintain the integrity of emergency call processes, ensuring availability of 99.999% at all network points (Ingress, Core, Egress). Key provisions include:

- The entire call path must be resilient and monitored for compliance with the availability standard.

Motorola Response

Comply.

- Support services not related to call handling should achieve an availability of 99.9%.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Resilience and monitoring of the entire call path for 99.999% availability at ingress, core, and egress with clear identification of any boundaries that are outside of the span of control of the contractor which may be a risk to achieving five nines (e.g., OSP ingress, PSAP egress). 99.9% availability is acceptable for non-call-handling support services.

Motorola Response

Comply.

The service provides 99.999% operational availability for the end-to-end 9-1-1 call path by employing a fully redundant and diverse architecture with no single point of failure. We utilize Active-Active multi-cloud architecture and redundant network edge infrastructure at each call handling system host location. For non-call-handling support services (e.g., administrative portals, non-critical reporting), we maintain a baseline of 99.9% operational availability.

The following boundaries are designated as outside our span of control

- **OSP Ingress:** The reliability of the OSPs network and the diverse local loop circuits provided by third-party carriers between the OSP and Motorola demarcation point defined at the POI.
 - **PSAP Egress:** The performance and availability of the PSAP call handling system beyond the demarcation point where the Motorola ESInet interfaces with the call handling system.
 - **GIS Data Integrity:** The accuracy and maintenance of the road centerline and address data, which remains the responsibility of the local 9-1-1 Authority.
-

- Uptime calculations assessing physical device MTBF for critical equipment in serial/parallel configurations.

Motorola Response

Comply.

Our reliability model assesses critical equipment (routers, BCFs, servers) using a combination of serial and parallel configurations.

By deploying these elements in parallel (redundant) pairs, the effective system availability is calculated as $A_{\text{total (parallel)}} = 1 - [(1 - A_1) \times (1 - A_2) \times \dots \times (1 - A_n)]$. For devices deployed in series, the total would be calculated as $A_{\text{total (series)}} = A_1 \times A_2 \times \dots \times A_n$.

Given that industrial-grade components in our core have a Mean Time Between Failures (MTBF) exceeding 100,000 hours.

- A comprehensive sparing plan for all sites with replacement strategies.

Motorola Response

Comply.

We maintain a Tiered Sparing Strategy to minimize downtime:

- **On-Site Spares:** Critical "consumable" components (SFPs, power cables, fans) are stocked at Core data center sites.
- **Regional Depots:** Complete hot-swappable units (e.g. SDWAN edge appliance) are maintained in regional Nebraska depots for rapid deployment.

- Replacement Strategy: We utilize a "Next Business Day" or "4-Hour On-Site" replacement lifecycle for all hardware under warranty, ensuring that once a redundant component fails, the primary/backup state is restored immediately.
-

- Established technician response times for outages.

Motorola Response

Comply.

We adhere to strict SLAs for technical response based on incident priority:

- Priority 1 (Mission Critical/Outage): 15-minute target response time; Hourly communications interval.
 - Priority 2 (Degraded/Loss of Redundancy): 30-minute target response time; Every 2 hour communications interval.
-

- Calculated MTTR based on spares and response times.

Motorola Response

Comply.

Our calculated MTTR is targeted at four (4) hour (maximum) response time to have a technician on-site for Critical or High Priority issue related hardware, software, network repair/maintenance issues or events. This includes all Holidays.

- A consolidated overview of overall availability combining MTBF and MTTR data.

Motorola Response

Comply.

Availability Overview: Combining a high MTBF (low failure frequency) with an aggressive MTTR (fast restoration), our consolidated system availability is mathematically modeled to provide the State with less than 5.26 minutes of downtime per year.

1.5.2 ESInet Reliability

The design of the ESInet must emphasize reliability through strategic diversity across geographic regions, technology, and vendors. Each node within the network must utilize **at least two routers from different manufacturers** to deliver redundancy. If this is unfeasible, a rationale for maintaining reliability under specific failure conditions must be provided. **No segment of the network should hinge on a single point of potential failure, such as a "backhoe incident."**

Motorola Response

Comply.

The reliability design must conform to guidelines specified in the FCC Report and Order 13-158 aimed at enhancing 911 reliability across all communication networks.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Strategic diversity across geographic regions, technology, and vendors.

Motorola Response

Comply.

Our proposed solution achieves strategic diversity by deploying a multi-vendor, multi-cloud, and multi-path architecture across distinct geographic regions. Our core NGCS elements are hosted in multiple geographically diverse, cloud data centers (e.g., Eastern, Central, and Western United States), ensuring that regional environmental disasters cannot disable the statewide system.

We employ a "Defense in Depth (DiD)" strategy by utilizing diverse transport technologies, including dedicated leased fiber, microwave backhaul, Low Earth Orbit (LEO) Satellite, and dark fiber, sourced from multiple independent telecommunications carriers where available, to ensure that a service disruption with one vendor does not impact the overall ESInet availability.

- Use of at least two routers from different manufacturers per node for redundancy (or rationale if unfeasible).

Motorola Response

Comply.

Our proposed ESInet is designed to use SD-WAN to securely connect 9-1-1 PSAPs, data centers, and service providers over multiple carriers, allowing traffic to be dynamically routed based on performance and priority. High Availability SD-WAN routers are deployed at site with dual routers, diverse circuits, and automatic failover so that voice, data, and emergency services continue without interruption service impacting events.

High Availability required the use of the same SD-WAN router manufacturer at each site. A single-vendor HA pair provides synchronized state, consistent failover behavior, and unified management. Using different router manufacturers introduces incompatible failover methods, adds complexity, and longer recovery times, reducing the reliability required for a mission-critical ESInet.

- Elimination of single points of failure (e.g., "backhoe incident").

Motorola Response

Comply.

Our service uses multiple network providers and diverse network architectures, including but not limited to MPLS, Broadband, LEO Satellite, or LTE, which eliminates single points of failure in the ESInet. If one carrier or technology fails, such as during a backhoe fiber cut, traffic automatically shifts to an alternate path, keeping 911 services available. These paths use different infrastructure and transport methods, providing true diversity and ensuring continuity of operations.

If a building has only one physical point of network entry, a single cut or failure can disconnect all services at once. Using multiple providers and architectures reduces this risk because each connection follows a different physical and logical path.

- Conformance to FCC Report and Order FCC 13-158 for enhancing 911 reliability.

Motorola Response

Comply.

The proposed ESInet and NGCS core conforms to the reliability mandates of FCC 13-158 for enhancing 9-1-1 reliability, including the requirement for annual reliability certifications. We implement all "reasonable measures" specified by the FCC, including:

- **Circuit Auditing:** Regular audits to verify physical circuit diversity and identify potential single points of failure.
- **Backup Power:** Ensuring all facilities supporting 9-1-1 routing have redundant, tested power systems (UPS and generators).
- **Network Monitoring:** Utilizing diverse monitoring links to our 24/7 NOC to ensure continuous observability of the 9-1-1 network state, as required by the FCC's reliability framework.

1.6 Operations and Management

1.6.1 ESInet Monitoring and Management

A dedicated 24/7/365 Network Operations Center (NOC) must oversee continual ESInet monitoring to ensure immediate detection of any functional disruption within the system. §E-9.3.1 contains minimum NOC requirements that must be met as part of this proposal.

- **All network links require constant congestion monitoring**, with timely mitigation strategies implemented by contractors.

Motorola Response

Comply.

- Failure alerts should be generated within a minute for any link or component malfunction of the ESInet.

Motorola Response

Comply.

Thresholds for triggering mitigation must be explicitly delineated, especially in response to network congestion, with proactive communication to the State regarding the mitigation plan, implementation timelines, and ongoing progress reports.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A dedicated 24/7/365 NOC for continual monitoring and immediate detection of disruptions.

Motorola Response

Comply.

Our dedicated NSOC provides 24/7/365 surveillance of the entirety of the proposed State's ESInet and NGCS core. Our NSOC is staffed by public safety technologists who utilize advanced event correlation and machine-learning algorithms to differentiate between minor network noise and mission-critical disruptions. This ensures that every functional element, from the ingress BCF to the SD-WAN devices at the call handling system host, are continuously monitored for hardware health, software application states, and link connectivity.

- Constant congestion monitoring of links with timely mitigation.

Motorola Response

Comply.

We perform real-time congestion monitoring on every ESInet link, utilizing SNMP and NetFlow telemetry to track bandwidth utilization and packet delivery success. If utilization on any primary or secondary route reaches a pre-defined "warning" state, our NSOC is alerted to perform dynamic traffic engineering. Mitigation strategies include the immediate re-prioritization of mission-critical SIP traffic via

SD-WAN orchestration and, if necessary, the activation of diverse overflow paths to ensure that 911 calls are never delayed by non-emergency data bursts or network congestion events.

- Failure alerts within 1 minute for malfunctions.

Motorola Response

Comply.

Our monitoring platform is engineered for sub-minute detection. When a critical functional element or network event occurs, the monitoring system generates a critical network alert at the NSOC in less than 60 seconds. This rapid-alert framework initiates an immediate automated triage process, notifying network engineers and triggering the failover logic required to maintain the 99.999% operational availability.

- Explicit thresholds for mitigation (e.g., congestion).

Motorola Response

Comply.

We establish clear, actionable performance thresholds that trigger automated and manual mitigation efforts:

- **Congestion Alert:** Triggered at 60% utilization sustained over 5 minutes; initiates investigation into traffic sources.
 - **Mitigation Action:** Triggered at 80% utilization; initiates automatic rate-limiting of non-critical administrative traffic and active load-balancing across diverse circuits.
 - **Critical Latency:** Triggered if one-way latency exceeds 50ms; initiates immediate path-reconvergence drills via BGP/BFD to shift traffic to a more optimal route.
-

- Proactive communication to the State on mitigation plans, timelines, and progress.

Motorola Response

Comply.

We maintain a Proactive Communication Protocol for all system-impacting events. Within 15 minutes of a confirmed Priority 1 incident, our NSOC provides the State with an initial Situation Report (SITREP) via the CWP and direct notification (email/SMS/Phone). We provide regular status updates every 30 to 60 minutes (based on incident severity) detailing:

- **Root Cause Analysis (RCA):** What triggered the event.
- **Mitigation Strategy:** Steps being taken to restore full service or redundancy.
- **Estimated Time to Restoration (ETR):** A projected timeline for final resolution and closure.

1.6.2 ESInet Maintenance Window

The proposed ESInet **must have no scheduled down time**. If maintenance is required, which would temporarily cause the network to have lower than 99.999% availability while the maintenance activity is underway, the contractor must provide a **pre-maintenance risk register** prior to commencing the maintenance and complete the maintenance under the terms of §E-9.5.1 (Change Management Requirements) and §E-9.5.2 (Scheduled Maintenance Process) below. **No maintenance activity which, if improperly completed, which could cause an outage of any part of the network, shall be permitted outside the terms of §E-9.5.1 and §E-9.5.2.**

Motorola Response

Comply.

All maintenance activity must be preceded by a Maintenance Operation Plan (MOP) required **at least 14 days** prior to the maintenance. The MOP shall include the provisional operating configuration to ensure that performance continually meets the 99.999% service level as the maintenance is being performed.

Motorola Response

Comply.

Scheduled downtime is unacceptable under routine operations. If maintenance is essential, it must follow as stringent Scheduled Maintenance Process to maintain or exceed 99.999% availability. Any maintenance that could jeopardize network functionality **must be strictly controlled.**

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- No scheduled downtime; completion of any maintenance impacting availability under specified terms (§E-9.5.1 and §E-9.5.2).

Motorola Response

Comply.

No scheduled downtime is required. We achieve this by utilizing an Active-Active geo-redundant architecture that allows maintenance to be completed without impacting availability.

Maintenance is performed on one core site at a time; traffic is seamlessly migrated to the peer site using BGP Graceful Restart and Session Persistence. The ESInet remains fully operational, and all activities comply with the Commission requirements in §E-9.5.1 and §E-9.5.2 for availability and outage mitigation.

- Prohibition of maintenance causing outages outside those terms.

Motorola Response

Comply.

Our Change Management methodology ensures that standard maintenance activities will not cause service outages.

We review every proposed update to ensure it can be executed using In-Service Software Upgrade or redundant pathing. Any activity that carries a risk of even momentary disruption is classified as "High Risk" and is only permitted during the State-approved maintenance windows with full fallback contingency plans in place.

- Requirement for a Maintenance Operation Plan (MOP) at least 14 days prior, including provisional configurations to maintain 99.999% service level.

Motorola Response

Comply.

For every scheduled maintenance activity, we will submit a detailed MOP to the State at least 14 calendar days in advance. Each MOP includes:

- **Provisional Configurations:** Step-by-step instructions for rerouting traffic to redundant nodes to maintain the 99.999% operations availability.
 - **Rollback Plan:** A defined Rollback Plan with validated procedures to restore the previous stable state within if any anomaly is detected.
 - **Impact Assessment:** A granular identification of the FEs involved and the verification tests to be performed post-maintenance.
-

- Descriptions of handling no-downtime requirements, planning/conducting maintenance without impacting availability, and the MOP process for guiding activities.

Motorola Response

Comply.

Our "No-Downtime" strategy is built around our defined Change Management process to carefully plan all engineer-led maintenance activities. Core NGCS services, including the ESRP, ECRF and ESInet, are updated in a controlled, rolling manner under the direct supervision of senior network engineers.

The Method of Procedure (MOP) process governs each activity and requires a lead engineer to review the plan with State stakeholders, confirms all provisional routing rules, and coordinate closely with the NOC for continuous monitoring. This deliberate, hands-on approach ensures maintenance is effectively a non-event for Nebraska's PSAPs, with no impact to 9-1-1 call delivery.

The MOP ensures that every system change, whether a software patch or a hardware upgrade, is executed with precision, transparency, and minimal risk. Managed under our broader Change Management framework, the MOP serves as a comprehensive, step-by-step roadmap for all maintenance activities.

MOP Lifecycle & Guiding Activities

1. Initiation & Documentation

We begin by defining the scope of the change. The MOP explicitly documents:

- **Logistics:** Specific timing, estimated duration, and required resources.
- **Accountability:** Clearly defined roles and responsible parties for each task.

2. Assessment & Planning

To ensure technical accuracy, every MOP undergoes rigorous validation:

- **System Check:** Confirmation against the current live system configuration.
- **Lab Validation:** Testing within the customer's lab environment (where applicable).
- **Risk Mitigation:** Development of a detailed contingency plan and a validated **back-out/rollback plan** to restore services immediately if needed.

3. Approval Process

Transparency is central to our delivery. Following internal technical reviews:

- **Submission:** The MOP is provided to the customer for final review and sign-off.
- **Compliance:** We adhere to customer-specific SLAs regarding lead times for MOP delivery prior to execution.

4. Implementation & Monitoring

During the maintenance window, the MOP acts as the primary governing document. Activities are executed in the recorded sequence, with real-time monitoring to ensure the system behaves as expected during and after the change.

5. Post-Implementation Review

Once the activity is complete, we verify system stability and document the outcome. This ensures that any lessons learned are captured to improve future maintenance cycles.

1.7 Implementation Details

1.7.1 Port Mapping

Comprehensive documentation of port block/mapping/forwarding policies must be maintained, providing access to both the State and PSAPs. This documentation should include provisions that allow stakeholders to request traffic on specific ports to be allowed from external sources into predetermined network points.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Comprehensive documentation of port block/mapping/forwarding policies accessible to the State and PSAPs.

Motorola Response

Comply.

We maintain a centralized Master Port and Firewall Policy document, which serves as the authoritative record for all allowed and denied traffic across the ESInet. This documentation provides a granular view of:

- **Standard i3 Ports:** Pre-configured paths for SIP (5060/5061), MSRP (text), and LoST/HTTP (routing) traffic.
- **Management Ports:** Restricted paths for SNMP monitoring, NTP timing, and SSH/VPN maintenance access.
- **Default-Deny Logic:** Documentation of our "Zero Trust" approach, where all ports not explicitly required for 9-1-1 operations are blocked by default at the BCF.

This documentation can be provided upon request, ensuring that the Commission administrators and PSAP IT personnel can review security configurations.

- Provisions allowing stakeholders to request traffic on specific ports from external sources to predetermined network points.

Motorola Response

Comply.

We have a formal Change Management process to accept requests from stakeholder needing to enable specific traffic flows (e.g., integrating a new third-party CAD vendor, Map data provider, or remote monitoring tool).

The process includes:

- **Request Submission:** Stakeholders submit a request via the Management Portal specifying the source IP, destination network point, port number/protocol, and business justification.
 - **Security Review:** Our security engineers will evaluate the request against NENA NG-SEC standards to ensure it does not introduce a vulnerability (e.g., ensuring requests use encrypted protocols like TLS).
 - **Implementation:** Once approved, the change is implemented via our standard Change Management process, ensuring the new port mapping is documented and synchronized across all redundant BCF nodes.
-

2. Next Generation Core Services (NGCS) Requirements

The proposal must include a Next Generation Core Services (NGCS) implementation deployed across multiple redundant data centers. The system shall use at least three (3) data centers, with a preference for at least one in-state and at least one geographically distant (more than 100 miles away – preferably several states away) to avoid common-cause failures such as severe weather or localized incidents. The state will permit a shared facility but prefers a separate NGCS instance (distinct virtual machines and management) from other tenants. Each NGCS component – physical and virtual – must be redundantly deployed in every data center with no single point of failure.

Motorola Response

Comply.

The NGCS must also be isolated and resilient against external threats and against faults arising elsewhere in the provider's NG911 ecosystem. Respondents must describe and demonstrate how their design prevents impact from incidents in another ESInet or statewide NGCS service offered by the provider, ensuring Nebraska's NG911 operations continue without degradation.

Motorola Response

Comply.

All NGCS elements which use policies must retrieve policies from a NENA-STA-010.3-compliant policy server and must be **provisioned with the host name of the policy server it uses**. See §E-2.2.1.1 for the NGCS Policy Store requirements.

- The State desires redundant functional elements, including all databases to be deployed active-active such that all redundant elements are actually serving traffic at all times.

Motorola Response

Comply.

- The Respondent must state which functional elements and databases are not actually serving traffic at all times and for each such element; the mechanism for failover that will reliably guarantee the 99.999% availability requirement of the entire system.

Motorola Response

Comply.

- **For active-active elements**, the Respondent must describe how the client determines an element has failed, and how it recovers (typically via retry), noting what the worst-case timing for the detection and retry is, and how the appropriate Service Level Objective within that SLA is maintained.

Motorola Response

Comply.

- **For each database**, and **each call-state data object**, the Respondent must describe how state is reliably maintained, and failover within the 99.999% availability is assured, including any retry operations required at the client.

Motorola Response

Comply.

- **For databases that are updated at call time**, the Respondent must describe the replication strategy, specify a maximum data sync time, and describe how it is achieved. Note that the State requires the ability to update a service boundary polygon in the ECRF dynamically, and replication/data sync of that operation must be described in the proposal.

Motorola Response

Comply.

- The State expects that the LPG, LNG, and MCS be the only element that supports legacy functions.

Motorola Response

Comply.

The contractor shall supply or ensure interoperability with all NGCS functional elements as defined by NENA, including but not limited to the Location Validation Function (LVF), Location Information Server (LIS), ECRF, Emergency Services Routing Proxy (ESRP), PRF, and Legacy Network Gateway (LNG). All elements must expose the NGCS interfaces specified in the standard, with the contractor documenting implementation details for each (e.g., integrated software modules, hosted cloud services, or third-party integrations). The system must support bridging to legacy systems via appropriate gateways.

Motorola Response

Comply.

All NGCS interfaces shall adhere to defined specifications, including SIP messaging extensions, RESTful APIs (using JSON/XML payloads), and NENA-defined ESInet ↔ Core interfaces. Payloads and schemas must comply with NENA requirements, such as Presence Information Data Format – Location Object (PIDF-LO) for location data, with support for HTTP-Enabled Location Delivery (HELD) protocols.

Motorola Response

Comply.

NGCS components (e.g., ECRF queries, LVF validations) must achieve performance targets, including lookup latency SLAs of 200 millisecond median and 500 milliseconds at the 95th percentile under peak load (jurisdiction may adjust based on scale). The system must handle at least 10 queries per second per component with no degradation.

Motorola Response

Comply.

The NGCS must scale horizontally to support jurisdiction-specific peak call rates (e.g., 1,000 calls per hour per PSAP) and data volumes, with tenant isolation for multiple PSAPs via virtual instances or containers. It shall enable dynamic provisioning of PSAP service boundaries through administrative interfaces.

Motorola Response

Comply.

All NGCS transactions shall be logged comprehensively, including timestamps, full request/response payloads (redacted for privacy where necessary), originator identities, correlation IDs, and error codes, enabling end-to-end tracing across components. Logs must be stored in a searchable database with retention support.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NGCS deployment in multiple redundant data centers (preference for at least 3, with one in-state and one >100 miles away).

Motorola Response

Comply.

Motorola complies with the requirement for a geo-diverse deployment of its NGCS). Motorola's Call Routing Service utilizes a highly resilient, multi-cloud architecture designed to provide national geographic diversity and ensure there is no single point of failure.

The geo-diverse deployment strategy includes the following key components:

- **Triple-Redundancy across Geographic Regions:** The NGCS FEs are distributed across a minimum of three distinct, geographically diverse cloud regions (e.g., East, Central, and West US) which are greater than 100 miles apart. This is an active, always-on strategy rather than just a passive backup.
 - **Multiple Cloud Providers:** To eliminate the risk of a single vendor's global software issue or hardware failure impacting the entire infrastructure, Motorola intentionally leverages at least two different cloud service providers. This ensures a service impacting event in one region is statistically non-correlated with the other two.
 - **Multiple Availability Zones:** Within each of the distinct geographic cloud regions, the system supports multiple Availability Zones to provide localized redundancy. This design ensures that the service impacting event in one Availability Zone will not disrupt the service within that region.
-

- Preference for separate instances (different VMs) if sharing data centers.

Motorola Response

Comply.

Motorola's Call Routing Service utilizes a highly resilient, multi-cloud architecture designed to provide national geographic diversity. Within each of the distinct geographic cloud regions, the system supports multiple Availability Zones to provide localized redundancy and redundant instances of NGCS functional elements within each zone. This design ensures that the failure of one Availability Zone will not disrupt the service within that region.

- Redundant deployment of all components without single points of failure; resistance to external threats and internal disruptions from other ESInets/NGCS.

Motorola Response

Comply.

The service is engineered with a "**Defense-in-Depth**" philosophy that ensures total operational isolation and component-level redundancy.

Zero Single Points of Failure: Every functional element (BCF, ESRP, ECRF, etc.) is deployed in a redundant, load-balanced configuration across multiple geographically diverse cloud regions. Our architecture utilizes Active-Active processing, where all components are simultaneously operational; if any individual server, switch, or entire data center experiences degradation, the remaining infrastructure absorbs the traffic without a restart or "warm-up" period, maintaining the 99.999% operational availability.

Resistance to External Threats: The system is hardened against cyber-attacks through Mutual TLS (mTLS) authentication and Session Border Control (SBC) at every ingress point. Our Network and Security Operations Center (NSOC) provides 24/7/365 monitoring, utilizing real-time intrusion detection and automated patch management to proactively neutralize malware, ransomware, and Distributed Denial-of-Service (DDoS) threats before they impact call processing.

Protection from Internal/Neighboring Disruptions: To prevent cascading network disruptions from other ESInets/NGCS, we implement logical network segmentation and service isolation. All Motorola NGCS FEs and services are containerized and hosted on multiple availability zones. This ensures that a traffic surge or technical disruption in a neighboring state's ESInet is isolated and cannot impact the Motorola service.

-
- Description/demonstration of unimpeded operation during disruptions.

Motorola Response

Comply.

The functional elements of the NGCS are implemented using a microservices architecture, where each element operates as an independent service across multiple availability zones. These geographically diverse regions are seamlessly interconnected through a sophisticated SDN IP network fabric, which dynamically optimizes traffic flows and ensures intelligent, fault-tolerant communication between the components ensuring no single point of failure.

The service architecture is designed for graceful and seamless failover. By leveraging an Active-Active multi-node deployment, any disruption to a single data center or network link triggers an instantaneous, automated shift of traffic to available nodes.

-
- Policy retrieval from NENA-STA-010.3-compliant policy server with host name provisioning.

Motorola Response

Comply.

Our service includes a NENA i3-compliant Policy Store that supports the storage of PRRs and standardized queries to the PRF. Policy retrieval leverages DNS to resolve the host name to locate its designated Policy Store.

- Preference for active-active redundant elements/databases serving traffic at all times.

Motorola Response

Comply.

The redundant NGCS FEs and databases are distributed across a minimum of three distinct, geographically diverse cloud regions and at least two different cloud service providers. This is an active-active, always-on strategy rather than just a passive backup.

We prioritize Active-Active deployment for all mission-critical elements (ESRP, ECRF, Databases), meaning all nodes serve live traffic simultaneously.

- Statements on non-active elements with failover mechanisms guaranteeing 99.999% availability.

Motorola Response

Comply.

The service utilizes an active/active architecture supporting 99.999% operations availability and does not include any non-active elements.

- Descriptions of failure detection/recovery for active-active elements (worst-case timing, SLO maintenance).

Motorola Response

Comply.

The service utilizes a sub-second heartbeat mechanism to monitor the health of all Active-Active FEs. In an Active-Active configuration, detection of a node failure occurs in less than 1 second via automated health probes. Because all nodes are actively processing traffic, recovery is near-instantaneous as the load-balancer or upstream element simply stops sending traffic to the failed node and redistributes the load among the surviving active nodes. We maintain a Service Level Objective (SLO) of 99.999% operational availability, ensuring that worst-case failover timing for call processing does not exceed 2 seconds.

- State maintenance/failover for databases/call-state data.

Motorola Response

Comply.

To prevent data loss during a site or component failure, we implement **distributed state management**. All call-state data—including the current status of a SIP dialog, the assigned dispatcher, and the active PIDF-LO location—is stored in a high-availability, clustered database environment.

In the event of a primary database node failure, a **coordinated failover** occurs where a secondary node is promoted to "Leader" status. This process ensures that the "state" of every 911 call is preserved, allowing any redundant ESRP to pick up a call mid-session without losing the audio path or metadata.

- Replication strategy for call-time updated databases with max sync time.

Motorola Response

Comply.

For databases that are updated in real-time (such as call logs and session information), we employ a Synchronous Replication Strategy within local clusters and Asynchronous/Near-Synchronous replication across geographic regions. Our solution guarantees a Maximum Sync Time of <100 milliseconds for local clusters, ensuring that data is committed to at least two physical nodes before a transaction is considered successful.

- Dynamic ECRF service boundary updates with replication/sync description.

Motorola Response

Comply.

The ECRF supports dynamic updates to service boundaries via the SI. When a GIS administrator publishes a new PSAP boundary or Emergency Service Boundary change, the SI pushes the update to all ECRF instances simultaneously. We utilize a Transactional Replication description where the ECRF validates the new GIS polygon data and swaps the active routing table in a "hitless" manner. This ensures that routing changes are reflected in real-time—ensuring calls are routed to the correct PSAP based on the newest map data—with a typical synchronization delay of less than 60 seconds across the entire statewide core.

2.1 Edge Security and Ingress

2.1.1 Border Control Function (BCF)

The BCF must conform to NENA-STA-010.3 standards, preferably constructed from a commercial Session Border Controller (SBC), Firewall, and NG911-specific capabilities.

Motorola Response

Comply.

- **Call Processing:** The BCF must handle all inbound calls from OSPs and should be configured between the ESInet and any interconnected ESInets to facilitate external connections.

Motorola Response

Comply.

- **Call Egress:** While optional, a BCF to manage outgoing communications between the ESInet and a PSAP may be necessary.

Motorola Response

Comply.

- **Security Features:** The BCF must incorporate the Bad Actor and Call Suspicion mechanisms as specified in NENA-STA-010.3. Calls directed to the ESInet should be accepted unless the source is blocklisted as a Bad Actor.

Motorola Response

Comply.

- **Media Handling:** The BCF must not anchor media unless it is necessary to do so. If the BCF does anchor media, it must implement ICE, STUN, and TURN mechanisms to navigate Network Address Translation (NAT) as applicable.

Motorola Response

Comply.

- **Logging and Monitoring:** The BCF must facilitate media logging per NENA-STA-010.3 specifications, with the ability to disable logging while retaining swift reactivation capabilities for diagnostic purposes.

Motorola Response

Comply.

The BCF must:

- Addresses on BCFs receiving traffic shall be globally routable IP addresses
- Process all calls from OSPs on the ingress side
- Support Bad Actor and Call Suspicion mechanisms
- Mitigate DDoS/TDoS attacks up to terabit capacity levels
- Accept calls directed to the ESInet regardless of source (unless marked as Bad Actor)
- Implement B2BUA if calls do not support REFER
- Avoid media anchoring where possible and implement ICE, STUN, and TURN when necessary
- Support ElementState and ServiceState SUBSCRIBE/NOTIFY

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 preferably from commercial SBC, Firewall, and NG911 capabilities.

Motorola Response

Comply.

The BCF is fully conformant with NENA-STA-010.3f and is built upon commercial-off-the-shelf (COTS) SBC and Firewall technology. Our implementation integrates specialized NG9-1-1 functional logic directly into the security stack, providing a single, hardened ingress point that handles SIP signaling, media policing, and deep packet inspection (DPI) to ensure that only valid emergency traffic enters the trusted core.

- Handling inbound calls from OSPs and between ESInets; optional egress BCF for outgoing to PSAP.

Motorola Response

Comply.

The BCF serves as the demarcation point for all inbound calls from OSPs and for inter-network traffic between Motorola call routing service and neighboring ESInets. The BCF provides ingress and egress protection for outgoing traffic to PSAPs. This ensures that even "last mile" delivery to the PSAP premise equipment is protected by the same rigorous security policies and mutual TLS (mTLS) authentication used within the core.

-
- Bad Actor/Call Suspicion mechanisms; acceptance of calls unless blocklisted.

Motorola Response

Comply.

We implement advanced **Bad Actor** and **Call Suspicion** mechanisms that evaluate incoming traffic patterns in real-time. The BCF is configured with an "Allow-by-Default" posture to ensure no legitimate 9-1-1 call is inadvertently dropped; however, it dynamically references Global and State-specific Blocklists. If a source is identified as a known malicious actor (e.g., TDoS botnets), the BCF will automatically throttle or block that specific traffic while keeping all other paths open for emergency requests.

- No media anchoring unless necessary with ICE/STUN/TURN for NAT.

Motorola Response

Comply.

In alignment with NENA standards, our BCF performs no media anchoring unless it is strictly necessary for security or protocol interworking. To support complex Network Address Translation (NAT) scenarios often found in OSP environments, the BCF supports the **ICE/STUN/TURN** framework. This allows for direct media paths between the caller and the PSAP whenever possible, reducing latency and core processing overhead while ensuring connectivity for devices behind restrictive firewalls.

- Media logging per standard with disable/reactivate capabilities.

Motorola Response

Comply.

The BCF provides standardized media logging as defined in NENA-STA-010.3. The gateway mirrors the media stream (audio, video, or RTT) to an authorized i3-compliant Logging Service for evidentiary and forensic use. For operational flexibility, authorized personnel can remotely **disable or reactivate media logging** on a per-session or per-interface basis via the secure management portal. This ensures that while logging is active by default to meet compliance, it can be suppressed for specific testing scenarios.

- DDoS/TDoS mitigation up to terabit levels.

Motorola Response

Comply.

Our BCF is engineered to protect the ESInet against large scale attacks. We implement multi-layered DDoS and TDoS mitigation that scales to terabit-per-second (Tbps) levels, ensuring the network remains resilient against massive volumetric floods.

Volumetric Defense: By utilizing high-capacity network "scrubbers" and distributed cloud-based mitigation, we can absorb and neutralize **DDoS** attacks exceeding 2.0 Tbps before they reach the core routing elements.

TDoS Protection: For Telephony Denial of Service (TDoS) attacks, the BCF employs **rate-limiting** and **behavioral analytics** to identify and drop suspicious signaling surges and malformed calls (e.g., botnet-generated calls) while prioritizing legitimate emergency traffic.

- B2BUA for non-REFER calls.

Motorola Response

Comply.

For all non-REFER call scenarios, the BCF operates as a Back-to-Back User Agent (**B2BUA**). This allows the BCF to maintain complete control over the SIP signaling and media state, enabling the network to bridge disparate SIP dialects and hide internal ESInet topologies from external entities, thereby enhancing the overall security posture of the NGCS core.

- ElementState/ServiceState support.

Motorola Response

Comply.

To ensure full observability, the BCF natively supports the **ElementState** and **ServiceState** framework. It provides real-time health telemetry to the NOC, including CPU/Memory utilization, active session counts, and security alert status. This data allows for proactive maintenance and immediate detection of any degradation at the network's edge.

- Descriptions of BCF locations, Bad Actor/Call Suspicion implementation, DDoS/TDoS capacity, B2BUA details, tromboning avoidance, ICE/STUN/TURN, media recording, and ElementState/ServiceState support.

Motorola Response

Comply.

BCF Location Strategy: The BCF is strategically deployed at the edge of the ESInet at every ingress point from OSPs. We deploy BCFs in a geographically diverse, triple-redundant configuration across our data centers (including Nebraska-based facilities). This ensures that traffic is sanitized and authenticated as close to the source as possible, preventing malicious or malformed traffic from ever reaching the NGCS core services.

Bad Actor and Call Suspicion Implementation: We implement a behavioral-based Call Suspicion mechanism that continuously analyzes traffic patterns for anomalies, such as rapid-fire call attempts from a single source or suspicious SIP header attributes. While the BCF operates on an "Accept-Unless-Blocklisted" policy to ensure no legitimate 9-1-1 call is lost. If a "Bad Actor" is identified, the system can automatically throttle that traffic or shunt it to a secondary inspection queue without impacting legitimate emergency requests.

DDoS/TDoS Mitigation Capacity: Our BCF features Terabit-level mitigation capabilities, designed to absorb and neutralize massive volumetric DDoS attacks reaching 1.0 Tbps and beyond. For TDoS, the BCF employs per-source rate limiting and SIP-level deep packet inspection to detect botnet behavior. This ensures that even during a concentrated cyber-assault, the Nebraska ESInet remains available for citizens in need.

B2BUA Details and Tromboning Avoidance: The BCF operates as a B2BUA for all non-REFER calls, which allows it to terminate an incoming SIP session and initiate a new one into the core. To prevent "tromboning" (where media unnecessarily loops through the core), the B2BUA facilitates direct media paths between endpoints once signaling is established. This optimization reduces latency and preserves core bandwidth, ensuring high-fidelity audio delivery.

NAT Traversal: ICE, STUN, and TURN: To ensure connectivity for mobile and VoIP callers behind restrictive firewalls, the BCF natively supports the ICE/STUN/TURN framework. The BCF acts as a TURN server when direct peer-to-peer media paths are blocked by symmetric NATs, providing a reliable relay point. This ensures that media—including voice and RTT—is successfully delivered regardless of the caller's local network configuration.

Media Recording Standards: In compliance with NENA-STA-010.3, our BCF supports standardized media mirroring to an external i3-compliant Logging Service. This recording includes all call media (audio, video, text) and associated metadata. Authorized administrators can enable, disable, or reactivate this logging on a per-session or per-port basis through the management portal, providing full control over evidentiary retention policies.

ElementState and ServiceState Support: The BCF provides real-time health and status updates using the ElementState and ServiceState framework. This telemetry is visible via the Motorola NGCS Portal, providing the State of Nebraska with immediate alerts on component health (ElementState) and overall service availability (ServiceState). This proactive monitoring ensures that any edge degradation is detected and mitigated within seconds.

2.1.2 STIR/SHAKEN Support

The State requires that incoming calls be validated, and the attestation results be supplied to PSAPs as specified in NENA-STA-010.3. Additionally, calls placed through the OCIF must be signed and receive A-level attestation when validated by the terminating service provider.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Validation of incoming calls with attestation to PSAPs per NENA-STA-010.3.

Motorola Response

Comply.

Our service provides full validation of STIR/SHAKEN digital signatures for all incoming SIP calls entering the ESInet. In accordance with NENA-STA-010.3f, our BCF and ESRP inspect the SIP Identity header to verify the attestation level (A, B, or C) provided by the OSP. This attestation information is then delivered to the PSAP CHE, allowing dispatchers to distinguish between verified callers and potentially spoofed or high-risk robocalls.

- Signing OCIF calls for A-level attestation.

Motorola Response

Comply.

For calls originated or managed within the ESInet, specifically those passing through the Outbound Call Interface Function (OCIF), we perform the "technological act" of signing the call. We ensure Full Attestation (Level A) for these calls by verifying that the calling identity is authorized and originated from a known, trusted source within the State's network. This ensures that emergency callbacks and outbound notifications from the PSAP are recognized as authentic by the public's wireless and wireline devices, preventing critical communications from being blocked as spam.

- Explanation of STIR/SHAKEN implementation/conformance.

Motorola Response

Comply.

Our STIR/SHAKEN implementation is a cloud-orchestrated solution integrated into the NGCS security stack. We act as a Service Provider in the STIR/SHAKEN ecosystem, maintaining valid registration in the FCC Robocall Mitigation Database (RMDB) and utilizing an authorized STI-CA (Certificate Authority) to manage secure tokens and certificates.

Our conformance strategy follows the NENA-INF-043.3 spoofing mitigation framework, providing:

- STI-VS (Verification Service): For real-time validation of incoming call signatures.
 - STI-AS (Authentication Service): For signing outbound/redirected calls with the appropriate PASSPorT headers.
 - Standardized Metadata: Delivery of verification status (e.g., "verstat") in the SIP header to the PSAP for clear display on the dispatcher's console.
-

2.1.3 Security Mechanisms

Until the PCA exists, the Contractor shall provide a Certificate Authority with a certificate traceable to a Certificate Authority trusted in mainstream browsers. All NGCS components must conform to NENA-STA-010.3 and NENA-STA-040.2 security requirements:

- All transactions across the ESInet (including local area network connections at NGCS sites) shall be encrypted as required in NENA-STA-010.3.

Motorola Response

Comply.

- Every entity must have credentials traceable to the PSAP Certificate Authority (PCA) as trusted root

Motorola Response

Comply.

- All TCP transactions must use TLS with mutual authentication

Motorola Response

Comply.

- Minimum cipher suite as specified in NENA-STA-010.3, with TLS 1.3 support required

Motorola Response

Comply.

- Server Name Indication support required in all systems

Motorola Response

Comply.

- All SIP "hops" within the ESInet must use TLS with mutual authentication

Motorola Response

Comply.

- Data access must conform to owner's Data Rights Management policy

Motorola Response

Comply.

- Single Sign On (SSO) mechanism with SAML authorization required

Motorola Response

Comply.

- No sharing of credentials permitted

Motorola Response

Comply.

- Public-facing connections require additional protection against security attacks

Motorola Response

Comply.

- JWS signatures required for policies and log events

Motorola Response

Comply.

- SIP transactions from OSPs at the BCF shall have appropriately strong minimum cipher suite.

Motorola Response

Comply.

- The Contractor shall notify the State if an OSP cannot support a cipher suite minimally acceptable to the Contractor.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 security with PCA-traceable credentials as trusted root.

Motorola Response

Comply.

The service fully conforms to NENA-STA-010.3f i3v3 security architecture, utilizing the PSAP PCA as the authoritative Trusted Root. All FEs are provisioned with digital certificates that are traceable to the PCA, ensuring that only authenticated devices and services can participate in the ESInet. This PCA-based hierarchy prevents unauthorized rogue elements from spoofing core services or intercepting call data.

- Mutual TLS for TCP transactions with minimum cipher suite and TLS 1.3 support.

Motorola Response

Comply.

We enforce Mutual TLS (mTLS) for all TCP-based transactions across the core. This requires both the client and server to present valid PCA certificates before a connection is established. To maintain a hardened posture, we support a minimum of TLS 1.2 with a strong preference for TLS 1.3. Our implemented cipher suites strictly exclude weak or legacy algorithms (like RC4 or 3DES), adhering to the following minimum standard:

- TLS 1.3: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256.
 - TLS 1.2: ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-GCM-SHA256.
-

- Server Name Indication support; TLS with mutual authentication for SIP hops in ESInet

Motorola Response

Comply.

Our solution natively supports Server Name Indication, allowing the core to securely host multiple virtualized services on a single IP address while maintaining certificate integrity. For SIP Hops within the ESInet, we enforce end-to-end security by requiring SIP-over-TLS with mutual authentication for

every signaling leg. This "Hop-by-Hop" security ensures that SIP signaling cannot be tampered with or eavesdropped on as it traverses the core from the BCF to the ESRP and finally the PSAP.

- Data access per owner's DRM policy.

Motorola Response

Comply.

Data access within the ESInet is governed by a robust Digital Rights Management (DRM) policy, ensuring that the State and local agencies remain the authoritative owners of their data. Access to sensitive records (e.g., call recordings, GIS layers, logs) is restricted based on specific owner-defined permissions, ensuring that only authorized personnel can view or retrieve data relevant to their jurisdiction.

- SSO with SAML authorization; no credential sharing.

Motorola Response

Comply.

To prevent unauthorized access and eliminate "password fatigue," we provide SSO utilizing the SAML 2.0 (Security Assertion Markup Language) standard. This integrates with the State's existing Identity Provider (IdP), allowing users to access all authorized ESInet applications with a single set of secure credentials. Credential sharing is strictly prohibited by both system policy and technical controls, ensuring that every action is uniquely attributable to a specific individual.

- Additional protection for public-facing connections.

Motorola Response

Comply.

For any interface exposed to the public internet (e.g., OTT messaging or web-based portals), we implement advanced protections including WAF (Web Application Firewall), rate-limiting, and Multi-Factor Authentication (MFA). These layers act as a buffer, neutralizing volumetric attacks and unauthorized intrusion attempts before they can reach the private ESInet core.

- JWS signatures for policies/log events.

Motorola Response

Comply.

Our proposed NGCS solution partially complies with this requirement by natively supporting strict JSON Web Signature (JWS) standards for our Logging Service, ensuring every LogEvent is securely packaged and stored as a Base64-encoded JWS.

Although our solution does not currently format all routing policies as signed JWS objects, full JWS integration for the Policy Store is actively scheduled on our engineering roadmap.

In the interim, all critical routing rules and access policies are strictly protected against unauthorized alteration through centralized Role-Based Access Controls (RBAC) and Zero Trust architectural boundaries. This strategy ensures uncompromised cryptographic protection for transactional log data today, alongside highly secure policy management as we transition to full JWS compliance.

-
- Descriptions of PCA implementation/traceability, TLS mutual authentication, cipher suite compliance, TLS

Motorola Response

Comply.

Our proposed NGCS solution utilizes a Public Key Infrastructure (PKI) rooted in the NENA PCA. All FEs are provisioned with digital certificates that are traceable to the PCA Trusted Root. This ensures that every node in the Nebraska ESInet can verify the identity and role of every other node. This traceability is critical for cross-ESInet interoperability, as it allows Nebraska to securely exchange 9-1-1 calls and data with neighboring states that also adhere to the national PCA trust model.

Mutual TLS (mTLS) Authentication Suggested Answer: We enforce Mutual TLS (mTLS) for all TCP-based transactions within the ESInet. Unlike standard TLS, where only the server proves its identity, mTLS requires both the client and the server to present and verify certificates. This two-way "handshake" ensures that no rogue device can initiate a connection to a core service, and no core service can be spoofed by an unauthorized actor, effectively neutralizing man-in-the-middle and credential-stuffing attacks.

Cipher Suite Compliance and TLS 1.3 Support Suggested Answer: Our solution strictly follows NIST SP 800-52 Rev. 2 guidelines for strong cryptography. We prioritize TLS 1.3 for all core communications to leverage its enhanced security and reduced handshake latency. To ensure cipher suite compliance, we only enable NIST-approved, FIPS-compliant algorithms that provide Perfect Forward Secrecy (PFS), such as:

- TLS 1.3: TLS_AES_256_GCM_SHA384 and TLS_CHACHA20_POLY1305_SHA256.
- TLS 1.2: ECDHE-RSA-AES256-GCM-SHA384 (as a fallback for legacy-compliant elements).

-
- 1.3 support, Server Name Indication, and SIP hop security.

Motorola Response

Comply.

We utilize the Server Name Indication (SNI) extension during the TLS handshake. This allows our virtualized core to host multiple secure services (e.g., separate ESRP or ECRF instances) on a single

IP address while ensuring the server always presents the correct certificate for the specific domain or service the client is requesting. SNI prevents "common name mismatch" errors and is essential for maintaining security in a modern, multi-tenant cloud environment.

SIP Hop Security Suggested Answer: Every "hop" of a SIP call within the ESInet is protected by SIP-over-TLS with mutual authentication. This means that the signaling path from the BCF to the ESRP, and from the ESRP to the PSAP, is fully encrypted and authenticated at each step. This Hop-by-Hop security ensures that sensitive SIP headers, including the caller's phone number and location data, are never transmitted in plain text and cannot be intercepted or modified as they traverse the network.

2.2 Core Routing and Location

2.2.1 Emergency Services Routing Proxy (ESRP)

The ESRP must conform to NENA-STA-010.3 standards and function as both originating and terminating ESRP. It shall be possible for a region or group of PSAPs to provide a terminating ESRP to which the State's ESRP must route calls to as appropriate.

Motorola Response

Comply.

The proposed solution must utilize the PRF functionality to support the ability to dynamically change the primary, alternate, and contingent routes available by the ESRP. The ESRP shall retrieve rule sets from a Policy Store using the NENA-STA-010.3 proscribed Policy Store web service. The ESRP must be capable of being provisioned to use any Policy Store conforming to NENA-STA-010.3. The ESRP shall implement the test call condition modifications described in NENA-STA-010.3 to enable automated testing of policy routing rules.

Motorola Response

Comply.

All calls must be location-routed with no ALI/MSAG-based routing. Requirements include:

- The ESRP shall be able to query any Location Information Servers using either HELD or SIP Presence.

Motorola Response

Comply.

- The ESRP shall support the QueueState and DequeueRegistration mechanisms for all queues it operates. It must support QueueState clients for queues for all PSAPs in the State.

Motorola Response

Comply.

- Policy Routing Rule function (PRF) supporting all NENA-STA-010.3 conditions and actions

Motorola Response

Comply.

- Policy retrieval from a Policy Store with dynamic updates (within 10 seconds)

Motorola Response

Comply.

- Handling at least 100 calls per second

Motorola Response

Comply.

- Support for admin calls

Motorola Response

Comply.

- Ability to query any compliant ECRF and Location Information Servers

Motorola Response

Comply.

- Support for call routing and EIDOs for any responder agency

Motorola Response

Comply.

- Implementation of overload and diversion mechanisms

Motorola Response

Comply.

- Additional Data mechanisms for routing based on call data

Motorola Response

Comply.

- ElementState and ServiceState support

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Conformance to NENA-STA-010.3 as originating/terminating ESRP.

Motorola Response

Comply.

Our proposed ESRP fully conforms with the NENA-STA-010.3f (i3v3) standard, functioning as both an Originating ESRP (receiving calls from OSPs) and a Terminating ESRP (delivering calls to PSAPs). It manages the full SIP signaling lifecycle, including session establishment, transfer, and termination, while ensuring that all signaling and media are handled through standardized i3 interfaces to maintain interoperability with other ESInets.

- Location-based routing only (no ALI/MSAG).

Motorola Response

Comply.

In strict alignment with the NG9-1-1 end-state, our ESRP performs location-based routing exclusively, eliminating the need for legacy ALI or MSAG tabular lookups. Every routing decision is based on a PIDF-LO (geospatial or civic). If an OSP does not provide a location, the system obtains it via our (LDB or dereferencing service at the time of the call, ensuring that the ESRP always has a valid location object to query the ECRF.

- PRF supporting all conditions/actions.

Motorola Response

Comply.

The ESRP utilizes an integrated PRF that supports a comprehensive set of conditions and actions as defined by NENA. This includes routing based on PSAP state (e.g., logged off, busy), time of day, call type (e.g., test, emergency), and service boundary. Actions supported include forwarding to a primary URI, diverting to an overflow queue, or rerouting to a secondary PSAP or Virtual PSAP based on predefined agency business rules.

- Policy retrieval from Policy Store with <10s updates.

Motorola Response

Comply.

Our ESRP retrieves and caches routing policies from a centralized i3-compliant Policy Store. The system is engineered to detect and apply policy changes, such as an emergency diversion manual trigger, in less than 10 seconds across all core nodes. This rapid synchronization ensures that when a PSAP supervisor updates their routing logic, the ESInet responds almost instantly to the new operational requirement.

- Handling 100 calls/second.

Motorola Response

Comply.

The ESRP is built on a carrier-grade, distributed architecture capable of sustained throughput of 100 calls per second (CPS) per node.

- Admin call support.

Motorola Response

Comply.

The VESTA NXT Router provides support for administrative calls in alignment with the NENA i3 standard for NGCS. Within the i3 architecture, administrative calls—such as those directed to a PSAP's traditional 10-digit number, multimedia calls, or a general SIP URI—are securely managed.

- Querying compliant ECRF/LIS.

Motorola Response

Comply.

Our proposed ESRP utilizes the LoST (Location-to-Service Translation) protocol to query any i3-compliant ECRF. For location acquisition, it interfaces with LIS or LDBs to ensure the most accurate PIDF-LO is used for the routing query. This adherence to standardized protocols prevents vendor lock-in and facilitates seamless cross-border routing.

- Routing/EIDOs for responder agencies.

Motorola Response

Comply.

Our proposed ESRP supports the creation and routing of Emergency Incident Data Objects (EIDOs). This allows the ESInet to transmit not just the call, but a rich data package including supplementary location, incident type, and responder-specific details to field agencies and secondary PSAPs. This ensures that the "intelligence thread" remains intact from the initial 9-1-1 call through to the dispatcher and the first responder's mobile device.

- Overload/diversion mechanisms.

Motorola Response

Comply.

To protect the integrity of the network, the ESRP includes automated Overload and Diversion controls. If a target PSAP exceeds its configured call capacity, the ESRP automatically invokes PRF rules to divert traffic to a pre-designated backup site. Additionally, the ESRP can perform SIP rate-limiting at the ingress to prevent a volumetric attack or mass-calling event from saturating core processing resources.

- Additional Data routing; and ElementState/ServiceState support.

Motorola Response

Comply.

The ESRP is designed to route "Additional Data" alongside the call session. Furthermore, it supports health telemetry through the ElementState and ServiceState framework. These states are reported to the Motorola NSOC, providing a real-time "heartbeat" of ESRP health and ensuring that any performance anomalies are detected and addressed before they impact public safety.

2.2.1.1 Policy Store

The State requires a Policy Store conforming to NENA-STA-010.3. The Policy Store must be capable of being the sole source of policies for the NGCS.

Motorola Response

Comply.

- The State **desires a flexible policy editor** that can create and modify policies conforming to NENA-STA-010.3 with an easy-to-use Graphical User Interface.

Motorola Response

Comply.

- The Policy Store **must have the capacity to support policies for all PSAPs and all elements in the NGCS** at the peak call rates specified in this RFS.

Motorola Response

Comply.

- Storage and retrieval of policies must be limited by the NENA-STA-010.3 Data Rights Management mechanism.

Motorola Response

Comply.

- The Policy Store must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Policy Store per NENA-STA-010.3 as sole policy source.

Motorola Response

Comply.

We will implement a centralized Policy Store as the sole, authoritative source of truth for the PRF, fully conformant with NENA-STA-010.3f (i3v3). The Policy Store holds all PRRs, including default routing, alternate routing (e.g., "Night Service"), and emergency diversion triggers. By centralizing these policies, we ensure that every ESRP across the geo-redundant core operates on an identical set of instructions, eliminating configuration drift and ensuring consistent call delivery.

- Flexible GUI policy editor.

Motorola Response

Comply.

Our NGCS CWP provides a flexible and user-friendly interface that allows authorized State and PSAP personnel to manage PRRs.

- Capacity for all PSAPs/elements at peak rates.

Motorola Response

Comply.

The Policy Store is engineered for mass-scale performance, designed to handle the peak transaction rates of all PSAPs and ESInet FEs simultaneously. Utilizing a distributed database back-end, the Policy Store can process thousands of policy queries per second with sub-millisecond latency. This high-capacity design ensures that even during a statewide emergency when multiple agencies may be simultaneously activating diversion plans, the Policy Store remains responsive and stable.

- DRM-limited storage/retrieval.

Motorola Response

Comply.

To ensure data sovereignty and security, the Policy Store employs Digital Rights Management (DRM) and RBAC. Policy storage and retrieval are strictly limited by agency ownership; for example, a PSAP supervisor can only view or modify policies belonging to their specific jurisdiction. All access is

authenticated via SAML-based SSO, and every retrieval or modification is logged with a non-repudiable audit trail, ensuring full accountability for routing changes.

- ElementState/ServiceState support with State subscription.

Motorola Response

Comply.

Our proposed NGCS solution fully supports the NENA-STA-010.3f "ServiceState" and "ElementState" framework, providing a standardized "heartbeat" for every component in the ESInet.

State Subscription: We provide a State-level Subscription Service that allows the State personnel to "subscribe" to the status of any FE or agency service. When an element (e.g., an ESRP) or a service (e.g., a specific PSAP's call delivery path) changes its operational state (e.g., from Normal to Degraded or Down), the system pushes an immediate notification to the State's monitoring dashboard and designated personnel. This proactive notification model ensures the State has 24/7 visibility into the health of the entire statewide network without needing to manually poll individual devices.

- Detailed Policy Store description.

Motorola Response

Comply.

Our Policy Store serves as the single, authoritative repository for all routing business logic. for the PRF.

NENA i3 Compliance: It is built on the NENA-STA-010.3f specification, ensuring that all policies are stored and retrieved using standardized format.

High-Performance Capacity: The Policy Store is designed as a geo-redundant, cloud-native cluster capable of handling peak transaction rates from all ESRPs and other FEs across Nebraska simultaneously, ensuring that even during mass-calling events, policy retrieval does not become a bottleneck.

DRM and Security: Access to policies is strictly governed by DRM and RBAC. Each agency maintains sovereignty over its own data; State-level users have broader visibility for coordination, while local PSAP users are restricted to their specific jurisdiction's routing logic.

2.2.2 Location Information Server (LIS)

The State utilizes a Location Information Server (LIS) provided by the existing service provider. Respondents must provide a description of their LIS solution in conformance with NENA-STA-010.3.

Motorola Response

Comply.

The LIS is the responsibility of the OSPs, but during transition Motorola will deploy an LDB) to insert location when the OSPs do not deliver location with the call. Motorola will also work with the OSPs and the PSAPs to move towards a full i3 solution to support OSP provided location delivery to the PSAPs removing the need for an LDB.

- The LIS must supply location in the form of a PIDF-LO (location by value) or a location URI (location by reference).

Motorola Response

Comply.

- The LIS must also provide a dereference service for a location URI it supplies given the URI, the LIS provides the location value as a PIDF-LO.

Motorola Response

Comply.

- A LIS may be a database, or may be a protocol interworking function to an access network-specific protocol.

Motorola Response

Comply.

- If the LIS supply's location by reference, it must also provide dereferencing service for that location URI.

Motorola Response

Comply.

- Elements in the ESInet, including the ESRP, and the PSAP may dereference a location URI as part of processing a call.

Motorola Response

Comply.

- The LIS must support HELD, HELD Dereferencing and/or SIP Presence Event Package.

Motorola Response

Comply.

- The SIP Presence SUBSCRIBE/NOTIFY mechanism can control repeated dereferencing, especially when tracking of the caller is needed. However, HELD is acceptable on any location URI.

Motorola Response

Comply.

- The LIS must support location filters and event rate control.

Motorola Response

Comply.

The LIS may support SIP Presence to provide location-by-reference as defined by RFC 5808. Using SIP Presence, the entity desiring location subscribes to the SIP Presence Event Package at the location URI provided containing a PIDF (Presence Information Data Format) document that will include the location in the Location Object (LO) part, forming the PIDF-LO.

Motorola Response

Comply.

- The LIS may validate locations prior to entering them into the LIS using the LVF.

Motorola Response

Comply.

- The LIS may support the validation of location around planned changes as defined by draft-ecrit-lost-planned-changes¹.

Motorola Response

Comply.

- The LIS must accept credentials traceable to the PCA for authenticating queries for a location dereference. Since calls may be diverted to any available PSAP, the LIS cannot rely on any other credential source to authorize location dereferencing.

Motorola Response

Comply.

- Storage and Retrieval of location data must be controlled by the NENA-STA-010.3 Data Rights Management mechanism

Motorola Response

Comply.

When location is provided by reference there is a need for the reference to be valid, at least for the length of the call. Since the call may be transferred to a transfer-to PSAP for handling, the transfer-to PSAP must have the ability to dereference the location reference provided with the call. It is therefore critical that the location URI does not expire before the transfer-to PSAP has the opportunity to dereference it.

Motorola Response

Comply.

Any LIS that provides a dereferencing service for a location must provide an expiration time associated with that URI set at a minimum of 30 minutes, with a maximum of 24 hours.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LIS per NENA-STA-010.3 providing PIDF-LO or location URI with dereference service.

Motorola Response

Comply.

The LIS is the responsibility of the OSPs and we expect the OSP provided LIS to comply with the NENA-STA-010.3 standard to support PIDF-LO or location URI with dereference service.

During transition Motorola will deploy a LDB to insert location when the OSPs do not deliver location with the call. Our LDB will provide PIDF-LO by value and by reference.

- As database or protocol interworking.

Motorola Response

Comply.

The LIS is the responsibility of the OSPs and we expect the OSP provided LIS to comply with the NENA-STA-010.3 standard.

- HELD/dereferencing/SIP Presence support.

Motorola Response

Comply.

The LIS is the responsibility of the OSPs and we expect the OSP LIS to provide HELD/dereferencing/SIP Presence support as defined in the NENA-STA-010.3 standard.

- Location filters/event rate control.

Motorola Response

Comply.

The LIS is the responsibility of the OSPs and we expect the OSP LIS to provide Location filters/event rate control as defined in the NENA-STA-010.3 standard.

- SIP Presence for location-by-reference per RFC.

Motorola Response

Comply.

The LIS is the responsibility of the OSPs and we expect the OSP LIS to provide SIP Presence for location-by-reference as defined in the NENA-STA-010.3 standard.

- Validation via LVF; support for planned changes draft.

Motorola Response

Comply.

The LIS is the responsibility of the OSPs and we expect the OSP LIS to support LVF validation and planned changes as defined in the NENA-STA-010.3 standard.

- PCA-traceable credentials for dereferencing.

Motorola Response

Comply.

The LIS is the responsibility of the OSPs and we expect the OSP LIS to support PCA-traceable credentials for dereferencing as defined in the NENA-STA-010.3 standard.

¹ <https://datatracker.ietf.org/doc/html/draft-ecrit-lost-planned-changes-00>

- DRM-controlled storage/retrieval; and minimum 30-min/max 24-hour URI expiration.

2.2.3 Location Database (LDB)

The State requires a Location Database (LDB) solution as a core component of the ESInet. Respondents must provide a detailed description of their LDB solution that is conformant with NENA standards, primarily the NENA Next Generation 911 GIS Data Model (NENA-STA-005.2). The LDB serves as the authoritative geospatial database for the Location Validation Function (LVF) and the ECRF.

Motorola Response

Comply.

During the transition to i3 Motorola's LDB is the primary source for ALI and MSAG data, whether legacy maintained or GIS-derived. It accepts various data formats, including NENA 2.1 standard ALI and MSAG formats. ALI records are verified against the legacy MSAG or GIS-derived MSAG to ensure validity before being used for location lookups. The LDB features a web interface for customers and service providers to view, manage records, and report discrepancies. The LDB will also generate records in the CLDXF format for those PSAPs where their GIS data contains both legacy and CLDXF attributes.

The SI is the authoritative source for GIS data, supporting functions like LVF, ECRF, and MCS. It processes data in various formats, such as NG9-1-1 GIS data, and exports it to NG9-1-1 components in required formats. This flexible SI implementation supports diverse methods of data maintenance and can provide data to systems that do not follow the NG9-1-1 GIS data model.

- The LDB must store and manage all mandatory and conditional geospatial data layers as specified in NENA-STA-005.2, including but not limited to:
 - Public Safety Answering Point (PSAP) Boundaries
 - Emergency Service Boundaries (Law, Fire, EMS)

- Road Centerlines
- Site / Structure Address Points

Motorola Response

Comply.

- The LDB must interface directly with the LVF to enable validation of civic location information against the authoritative GIS data contained within it.

Motorola Response

Comply.

- The LDB must interface with the ECRF to provide the necessary geospatial data for determining the appropriate PSAP and emergency service agencies for a given dispatchable location. This location-to-service mapping **MUST** utilize a standard protocol, such as the Location-to-Service Translation (LoST) protocol.

Motorola Response

Comply.

- The solution must provide a secure and robust mechanism for the provisioning, aggregation, and ongoing maintenance of GIS data from various authoritative local sources (e.g., county, and municipal GIS departments). This includes tools for data normalization, quality control, and discrepancy resolution.

Motorola Response

Comply.

- The LDB must be architected for high availability and geographic redundancy to ensure uninterrupted location validation and call routing services. The system must meet stringent performance requirements for real-time query processing during emergency call handling

Motorola Response

Comply.

- The LDB must control access for data provisioning and system queries through secure authentication and authorization mechanisms, protecting data from unauthorized access, modification, or deletion.

Motorola Response

Comply.

- Storage, management, and retrieval of location data MUST be controlled by policies consistent with NENA data security and privacy standards.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- LDB conformance with the NENA-STA-005.2 GIS Data Model.

Motorola Response

Comply.

The LDB is the primary source for ALI and MSAG data, whether legacy maintained or GIS-derived. It accepts various data formats, including NENA 2.1 standard ALI and MSAG formats. ALI records are verified against the legacy MSAG or GIS-derived MSAG to ensure validity before being used for location lookups. The LDB features a web interface for customers and service providers to view, manage records, and report discrepancies.

The SI is the authoritative source for GIS data, supporting functions like LVF, ECRF, and MCS. It processes data in various formats, such as NG9-1-1 GIS data, and exports it to NG9-1-1 components in required formats. This flexible SI implementation supports diverse methods of data maintenance and can provide data to systems that do not follow the NG9-1-1 GIS data model.

- Standard-based interfaces with the LVF and ECRF (e.g., LoST).

Motorola Response

Comply.

The interfaces for the ECRF and the LVF are fundamentally built upon NENA i3 standards (such as NENA-STA-010.3e-2021) and rely heavily on the LoST protocol (specifically RFC 5222).

- Support for all required NENA GIS data layers and their lifecycle management.

Motorola Response

Comply.

The service utilizes all critical NG9-1-1 GIS data layers necessary for geospatial routing and civic address validation, including Site/Structure Address Points, Road Centerlines, PSAP Boundaries, and Emergency Service Boundaries (Law, Fire, EMS). Other layers may be uploaded to the SI if additional outputs are needed for PSAP or CAD mapping exports.

Authoritative GIS data is provisioned via the SI, which acts as the backbone for managing the flow of geographic data into the NGCS elements. The SI automatically performs geometry, attribution quality, and integrity checks supporting NENA-STA-006, NENA-STA-015, and NENA-STA-010 standards. Once these rigorous checks pass, the SI transforms the datasets projection and schema into the necessary formats and seamlessly provisions the data to both the ECRF and LVF databases.

The SI does allow rollbacks to previously provisioned data should valid, but erroneous data be provisioned to the ECRF/LVF.

- A detailed process for GIS data provisioning, aggregation, updates, and quality control.

Motorola Response

Comply.

The SI enables users to upload data via a web portal at any frequency they prefer. Submitted data undergoes thorough validation to check field consistency, attribute accuracy, and geometry validity. If errors are detected, an error database is generated for users to download and resolve inconsistencies.

The system supports independent data uploads from multiple agencies, including third parties, and aggregates the data. It then performs additional validations along boundaries to ensure the final output is uniform and error-free.

- Description of the high-availability and redundant architecture.

Motorola Response

Comply.

The LDB is integrated as a core functional element within Motorola's NGCS and is deployed across a **redundant and geographically diverse multi-cloud infrastructure**. To achieve maximum high-availability, the LDB architecture incorporates the following features:

- **Geographic and Local Redundancy:** The LDB is hosted in a multi-cloud environment using a microservices architecture, operating as an independent service across multiple availability zones.
- **No Single Point of Failure:** By distributing the LDB and other FEs across multiple interconnected and highly secure Availability Zones, the architecture is engineered to eliminate any single point of failure.

- **Redundant Database Instances:** The NGCS system actively maintains and updates **redundant database instances** to ensure continuous data synchronization and operation.
-

- Mechanisms for secure access control for both data management and system queries.

Motorola Response

Comply.

Our mechanisms for secure access control are built on a zero-trust architecture and the **principle of least privilege**, ensuring that systems and personnel are configured with only the minimum applications, permissions, and access rights necessary to fulfill their specific roles.

We secure data management and system queries through the following multi-layered mechanisms:

Strong Authentication and Credentialing

- **MFA:** MFA is supported and required for any external access to our web portals and user interfaces, including the PRF portal, GIS SI, reporting portals, system dashboards, and the LDB.
- **Two-Factor VPN Access:** All remote system access utilizes a highly secure Virtual Private Network (VPN) that requires two-factor authentication. This ingress is tightly controlled and monitored in real-time by the NSOC.
- **Strict Password Policies:** We enforce robust authentication policies that require complex passwords (incorporating uppercase, lowercase, numerals, and special characters), prevent the use of dictionary words or easily guessed sequences, mandate regular expirations, and automatically lock out users after five invalid login attempts.

Role-Based Data Management

- **Granular Permissions:** Access to data management tools is strictly governed by defined roles and responsibilities. For example, the secure web interface for the LDB allows administrators to customize credential rights; database coordinators can be granted full access to edit ALI and MSAG records, while local addressing authorities might only be given "view-only" permissions to suggest updates without altering the live data.
- **Secure Data Uploads:** Spatial data is managed through the secure SI portal, which tracks the specific authorized entities uploading GIS datasets and validates the integrity of the data before it is provisioned into the live routing environment.

Partitioned System Queries and Reporting

- **Multi-Tenant Partitioning:** System queries and historical reporting are managed in a multi-tenant environment. Transactional logs and i3 events are partitioned based on user role, call type, specific PSAP, or agency jurisdiction. This ensures that when personnel run queries or generate reports, they only have access to the data relevant to their authorized geographic area or clearance level.

System-to-System Access and Encryption

- **Encrypted Communications:** We utilize TLS and industry-standard encryption algorithms (including AES-256) across all connections to external entities to ensure the confidentiality and integrity of all transmitted data and queries.

- **Continuous Authentication:** When system-to-system access is implemented (such as continuous connections or push technology), the source system is strictly authenticated before each transfer session, and the system is designed to never mask individual accountability for these transactions.
 - **Digital Certificates:** All components, FEs, and PSAP interconnections rely on Digital Certificates tied to our ICA to ensure identity verification and a secure chain of trust.
-

- Tools and processes for managing data quality and resolving discrepancies from multiple sources.

Motorola Response

Comply.

The LDB features a web interface for collaboration between customers, service providers, and Motorola staff to review data within the LDB. It also enables users to report discrepancies, which can be assigned to the appropriate service provider for resolution.

2.2.4 Emergency Call Routing Function / Location Validation Function (ECRF/LVF)

The implementation requires two independent, redundant ECRFs and LVFs (one inside, one outside the ESInet) with identical data. The ECRF/LVF must support the extensions to LoST defined in NENA-STA-010.3 and the similar-location and planned-changes extensions defined in draft-ietf-ecrit-similar-location² and draft-ietf-ecrit-lost-planned-changes³ (or RFCs issued based on those drafts).

Motorola Response

Comply.

Query Capability:

² <https://datatracker.ietf.org/doc/draft-ietf-ecrit-similar-location/19/>

³ <https://datatracker.ietf.org/doc/draft-ietf-ecrit-lost-planned-changes/>

The external ECRF/LVF must be queryable from the public internet and by any i3 OSP, supporting both iterative and recursive queries.

Motorola Response

Comply.

Responder Types:

The system must handle up to 20 responder types and various service URNs as specified.

Motorola Response

Comply.

Data Synchronization:

Both the internal ECRF and LVF must achieve 99.999% availability, while the external ECRF must meet the same 99.999% availability SLA, and the external LVF must maintain 99.9% availability.

Motorola Response

Comply.

Performance Metrics:

- The internal ECRF/LVF must handle 500 queries per second effectively, ensuring that combined services meet the specified thresholds for external queries.

Motorola Response

Comply.

Key requirements:

- External ECRF/LVF accessible from the public Internet and i3 OSPs

Motorola Response

Comply.

- Support for iterative and recursive queries

Motorola Response

Comply.

- Support for up to 20 responder and all service URNs

Motorola Response

Comply.

-
- LoST sync interface to National Forest Guide and interconnected ESInets

Motorola Response

Comply.

- The ECRFs and LVFs must be capable of being provisioned from an SI conforming to NENA-STA 010.3.

Motorola Response

Comply.

- Routing/validation must change within eight (8) seconds of an update via the SI.

Motorola Response

Comply.

- The internal ECRF/LVF shall be capable of handling 100 queries per second for any valid Location Information shape as specified in OGC 06-142r1.

Motorola Response

Comply.

- The external ECRF/LVF shall be capable of handling an aggregate of 5000 queries per second with any mix of civic or geo points.

Motorola Response

Comply.

- The external ECRF/LVF shall be capable of handling an aggregate 500 queries per second.

Motorola Response

Comply.

- The external ECRF/LVF shall limit transactions from the same querier to, at most, 10 per second and fewer, if it is under a sustained excessive load. If the ECRF and LVFs are combined, the combination must meet the 5000/500 rate (not twice the rate of a single service).

Motorola Response

Comply.

- 99.999% availability for internal ECRF/LVF and external ECRF

Motorola Response

Comply.

- 99.9% availability for external LVF

Motorola Response

Comply.

- Support for Spatial Interface (SI) with routing/validation updates within seconds

Motorola Response

Comply.

- Capacity to handle specified query volumes

Motorola Response

Comply.

- ElementState and ServiceState support

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Two independents are redundant ECRFs/LVFs (internal/external) with identical data.

Motorola Response

Comply.

Motorola's internal and external ECRF/LVFs are geo-redundant and designed for high availability. They use the same data supplied through the SI to maintain accuracy and consistency.

- External queryable from public Internet/i3 OSPs with iterative/recursive support.

Motorola Response

Comply.

Motorola's internal and external ECRF/LVFs are geo-redundant and designed for high availability. They use the same data supplied through the SI to maintain accuracy and consistency.

- Handling up to 20 responder /service URNs; LoST sync to National Forest Guide/interconnected ESInets.

Motorola Response

Comply.

The LoST interface supports unlimited service URNs embedded in GIS data, enabling it to handle all responder boundaries defined in NENA STA-010.3 and accommodate future additions. It can integrate with the National Forest Guide and perform LoST sync to locally store coverage boundaries, reducing reliance on the forest guide for recursive queries.

- 99.999% availability for internal/external ECRF and internal LVF, 99.9% for external LVF.

Motorola Response

Comply.

The LoST interface, both internal and external, are geo-redundant and highly available, meeting the need for 99.999% operational availability for the overall service.

- SI support with seconds-level updates.

Motorola Response

Comply.

The SI supports near real-time processing of changes made to authoritative GIS databases. The SI will immediately pass through, to the ECRF/LVF, all valid features while holding back those with critical errors for remediation by the provider.

- Capacity for 500 queries/second internal; and ElementState/ServiceState support.

Motorola Response

Comply.

The LoST service is highly scalable, capable of handling more than 500 queries/second for both civic and geodetic queries as required by the RFP. It includes support for ElementState and ServiceState to monitor overall system performance and maintain uptime metrics.

2.2.5 Forest Guide

The NGCS must handle calls transferred between interconnected ESInets, maintaining Forest Guide entries for the State's ECRF and LVF, and support recursive queries for locations outside the state's service area.

Motorola Response

Comply.

If a National Forest Guide is available, the contractor must ensure the State's ECRF and LVF entries are entered promptly.

Motorola Response

Comply.

Fallback Procedures:

In scenarios where queries fall outside the State's service area, the ECRF/LVF must initiate recursive queries to the Forest Guide.

Motorola Response

Comply.

Commercial Relationships:

Frequent and excessive queries from the same entity may not be accommodated unless a reasonable commercial relationship exists.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Handling transfers between ESInets with Forest Guide entries for State's ECRF/LVF.

Motorola Response

Comply.

Motorola will work with neighboring ESInet providers to determine accessibility to PSAPs. Should the Forest Guide and ECRF return a destination to a neighboring PSAP, the ESRP will deliver the call to the destination.

- Recursive queries for out-of-area locations.

Motorola Response

Comply.

Motorola's LoST interface supports hierarchical LoST servers, enabling the system to prioritize local, regional, or state-level servers over the Forest Guide.

- Prompt entry into National Forest Guide if available.

Motorola Response

Comply.

Motorola is dedicated to provisioning coverage areas in the National Forest Guide once available.

- Fallback recursive queries to Forest Guide for non-State areas.

Motorola Response

Comply.

Motorola's LoST interface supports hierarchical LoST servers, enabling the system to prioritize local, regional, or state-level servers over the Forest Guide. However, in the event the local, regional or state-

level servers cannot provide an authoritative answer, the system will utilize the National Forest Guide to retrieve the authoritative LoST server to query.

- Limitations on excessive queries without commercial relationships.

Motorola Response

Comply.

The LoST interface is designed to prevent unwarranted clients from querying the service in excess. Rate limiting can be deployed as a deterrent mechanism in the event the system is becoming overloaded with queries.

2.2.6 Service/Agency Locator (SAL)

The State requires a Service/Agency Locator function as described in NENA-STA-010.3.

- The S/AL must support at least 1000 entries.

Motorola Response

Comply.

- The S/AL must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.

Motorola Response

Comply.

- The proposal must describe how agency entries are provisioned in the S/AL.

Motorola Response

Comply.

S/AL records are managed through a secure web-based interface or via automated API integration that enables adding, updating, and deleting records. Each entry undergoes validation to ensure URI formatting and service tags align with NENA standards before being committed to the active directory.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Service/Agency Locator per NENA-STA-010.3 supporting 1000+ entries.

Motorola Response

Comply.

The S/AL record store can hold an unlimited number of records for any given agency.

- ElementState/ServiceState support with State subscription.

Motorola Response

Comply.

The S/AL generates an elementStateLogEvent to enable loggers to monitor the state of the functional element and can also subscribe to ServiceState, which is essential for assessing system availability.

- Descriptions of agency entry provisioning and detailed S/AL.

Motorola Response

Comply.

Users manage records in the S/AL record store via a secure web-based portal with MFA. Provisioned data can be searched within the portal and is instantly accessible through the S/AL API. Systems accessing the API via the public internet use mTLS secured with certificates linked to the credentialing agency.

2.3 Data and Enrichment

2.3.1 Additional Data Repository (ADR)

The State requires an Additional Data Repository (ADR) database function.

URIs pointing to the ADR may be passed in a call, in an EIDO, or by other mechanisms. The ADR shall return an XML data structure in response to an HTTPS GET of the URI.

Motorola Response

Comply.

The ADR provided by the contractor must:

- Supply Provider Info and Service Info for all calls handled by the LNG, and any OSP that does not provide its own ADR or AdditionalData by value when it sends a call to the ESInet

Motorola Response

Comply.

- Supply any of the valid AdditionalData blocks for any location, where the URI for the AdditionalData blocks would be returned from the ECRF when searched with an urn of "urn:emergency:service:AdditionalData"

Motorola Response

Comply.

The proposal must detail how ADR records are provisioned into the repository. Storage and retrieval of S/AL records must be controlled by the NENA-STA-010.3 Data Rights Management mechanism.

Motorola Response

Comply.

A call-stateful ADR may limit the length of time that it will serve data after the end of the associated emergency call. Such a time limit shall be at least five minutes. ADRs may not have the data themselves but may know where the data can be found. The response to a dereference request can be redirected to another ADR with an HTTPS 333 response (Iterative Refer).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- ADR returning XML via HTTPS GET.

Motorola Response

Comply.

Motorola's ADR information blocks are retrieved through HTTP(s) GET requests and return XML objects as defined by NENA-STA-010.3 and RFC 7852.

- Supplying Provider/Service Info for LNG/OSPs without own ADR.

Motorola Response

Comply.

Motorola's LDB supports ADR for ProviderInfo, ServiceInfo, SubscriberInfo and Comment data blocks. This data is provisioned through SOI update processing and linked to the appropriate NENA-STA-010.3 ADR fields. Additional information is updated in the ADR through the e2 interface to provide information such as the callback number in SubscriberInfo.

- Valid Additional Data blocks via ECRF URI.

Motorola Response

Comply.

Motorola supports querying the ECRF for additional data which is stored in the Address Points Additional Data URI field.

- Provisioning details.

Motorola Response

Comply.

Motorola's LDB supports ADR for ProviderInfo, ServiceInfo, SubscriberInfo and Comment data blocks. This data is provisioned through SOI update processing and linked to the appropriate NENA-STA-010.3 ADR fields. Additional information is updated in the ADR through the e2 interface to provide information such as the callback number in SubscriberInfo.

- DRM-controlled storage/retrieval.

Motorola Response

Comply.

Additional data control mechanisms are in place to ensure only authorized users can access the information.

- Minimum 5-minute time limit for call-stateful ADR.

Motorola Response

Comply

The LDB ADR component allows for ADR retrieval throughout the lifetime of the call and a minimum grace period of 5 minutes to ensure the information can be retrieved.

- Redirect capability via HTTPS 303.

Motorola Response

Comply.

Motorola's LDB acting as an ADR contains all the information needed to support the retrieval of ALI associated data and does not need to refer to another ADR.

Motorola supports external ADRs' ability to redirect via HTTPS 303 to other URLs.

2.4 Call Flow and Media Handling

2.4.1 Call Flow and Session Handling Requirements

The Contractor shall implement call-flow behaviors consistent with the NENA i3 call model, including processing SIP INVITE requests from access networks into the ESInet, interactions with the ESRP, location queries to LIS, LVF, and ECRF, and routing to the appropriate PSAP through gateways or Call Handling Equipment (CHE). The system must support call queuing, overflow routing, and abandonment handling.

Motorola Response

Comply.

SIP signaling and location:

Headers such as P-Asserted-Identity, Diversion, History-Info, and Geolocation shall be correctly handled, and PIDF-LO location information shall be preserved during retargeting, bridging, and transfers.

Motorola Response

Comply.

Media and additional data:

The system shall handle voice, Real-Time Text (RTT), real-time video, and additional data (for example, messaging and sensor or biometric data from caller applications) per NENA definitions, with SDP negotiation, fallback to voice-only, and transcoding as needed.

Motorola Response

Comply.

Transfers:

Support is required for warm (attended) transfers, blind transfers, and inter-PSAP transfers, preserving all call metadata, location, timestamps, and media sessions without interruption.

Motorola Response

Comply.

Identity and trust:

The system shall enforce SIP identity assertions, correctly process P-Asserted-Identity and related headers, differentiate and display validated versus unvalidated identities at the PSAP, and integrate with STIR/SHAKEN for caller authenticity.

Motorola Response

Comply.

End-to-end conformance:

The ESInet and NGCS shall manage end-to-end call flows in conformance with applicable NENA and IETF standards, including origination, routing, delivery to the appropriate PSAP, transfers, and termination, while ensuring reliable session handling for all supported media.

Motorola Response

Comply.

2.4.2 Media Quality of Service (QoS)

2.4.2.1 Audio

The proposed solution shall support high-quality, reliable audio for all emergency calls. The solution must be conformant with NENA and IETF standards for audio codecs and media transport to ensure interoperability between originating networks, the ESInet, and PSAPs.

Motorola Response

Comply.

- MOS-equivalent POLQA score of 4 minimum, 4.5 average from OSP edge to PSAP edge

Motorola Response

Comply.

- Continuous sampling of >1% of calls randomly distributed

Motorola Response

Comply.

- Capability to monitor 100% of calls between any two points for up to 5 days upon request

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- High call quality with audio MOS-equivalent POLQA score of 4 minimum/4.5 average from OSP to PSAP edge.

Motorola Response

Comply.

We commit to delivering high call quality audio with a POLQA (ITU-T P.863) score of 4.0 or higher and maintaining a statewide average of 4.5. To achieve this, our ESInet utilizes specialized QoS policies, media policing and jitter buffer management at the BCF, ESRP and across the ESInet. By utilizing the G.711 codec and enforcing strict DSCP marking, we minimize packet loss and latency, which typically degrade MOS scores in standard IP networks.

- Continuous sampling >1% of calls; capability to monitor 100% of calls between points for up to 5 days.

Motorola Response

Comply.

Our QoS monitoring engine provides dual-mode surveillance of the media stream:

Standard Sampling: The system performs continuous sampling of >1% of all calls to establish a baseline for network-wide audio performance.

Targeted Deep Monitoring: On-demand or during troubleshooting, the system can scale to monitor 100% of calls between specific network points for a duration of up to 5 days. This granular data capture allows our engineers to perform deep packet analysis on specific traffic legs to identify transient network issues or OSP-side quality issues.

- Descriptions of end-to-end media path measurement, POLQA monitoring/measurement, and logging/reporting procedures.

Motorola Response

Comply.

We utilize an active and passive monitoring strategy to measure the end-to-end media path.

Measurement: We deploy virtual probes at critical handoff points, ingress (BCF), core (ESRP), and egress (PSAP-side router). These probes measure Real-time Transport Protocol (RTP) statistics, including jitter, latency, and packet loss, which are then correlated into the POLQA-equivalent score.

Logging and Reporting: All QoS metrics are logged and made available in the NGCS CWP. Authorized State personnel can access automated weekly or monthly reports that aggregate these scores, providing clear visibility into whether the service is meeting the voice quality standards.

Alerting: If any call leg drops below the 4.0 POLQA threshold, the NSOC receives an immediate "Minor" alert, allowing for proactive investigation before the quality degradation becomes perceptible to telecommunicators.

2.4.2.2 Video

For video services, the proposed service must utilize MOS-equivalent PEVQ score of 4 minimum, 4.5 average from OSP edge to PSAP edge, and have continuous sampling of >1% of calls randomly distributed. They should also have the capability to monitor 100% of video calls between any two points for up to 5 days upon request.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Video MOS-equivalent PEVQ score of 4 minimum/4.5 average from OSP to PSAP edge.

Motorola Response

Comply.

We commit to a video quality standard using the PEVQ (ITU-T J.247) algorithm, ensuring a minimum score of 4.0 and maintaining a statewide average of 4.5. Unlike standard bitstream analysis, our PEVQ

implementation performs a perceptual evaluation that accounts for blockiness, jerkiness, and frame freezes. This ensures that even when a caller is streaming from a low-bandwidth cellular area, the ESInet core optimizes the delivery path to maintain the highest possible picture quality at the PSAP

- Continuous sampling >1% of calls.

Motorola Response

Comply.

We perform continuous sampling of >1% of all video sessions entering the ESInet to ensure regional quality baselines are met.

- Capability to monitor 100% of video calls between points for up to 5 days; and descriptions of end-to-end video path measurement, PEVQ monitoring/measurement, and logging/reporting procedures.

Motorola Response

Comply.

We employ a multi-layered approach to measure and report on the video path:

Measurement: We utilize virtual probes that analyze RTCP reports and perform DPI on the video stream. These probes measure KPIs such as effective frame rate, lip-sync delay (audio/video synchronization), and temporal activity.

PEVQ Scoring: The system compares the degraded video received at the PSAP against the reference stream at the ingress point (BCF) to calculate the PEVQ MOS.

Logging & Reporting: All metrics are logged in the NGCS Portal, allowing State administrators to generate detailed reports on video performance. If a video session's quality falls below the 4.0 threshold, the Network and NSOC is automatically alerted to investigate potential network congestion or hardware bottlenecks.

2.4.2.3 Text

The State requires that text to 911 and text from 911 be supported for both legacy and NG PSAPs and OSPs.

- For NG911, text to 911 shall be provided via Message Session Relay Protocol (MSRP) using standard NENA-STA-010.3 interfaces.

Motorola Response

Comply.

- For text from 911, Contractor shall maintain an interface to a commercial text gateway.

Motorola Response

Comply.

- For Legacy PSAPs, MSRP or web interfaces to the outgoing text service are required.

Motorola Response

Comply.

Text from NG PSAPs shall be able to send MSRP to an element in the NGCS which will send SMS text using the text gateway.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 100% correct text delivery 99.99% of the time.

Motorola Response

Comply.

We provide the delivery of Text-to-911 through a "delivery receipt" and "session persistence" model. To achieve 100% correct text delivery 99.99% of the time, our ESInet utilizes the MSRP Message Session Relay Protocol (MSRP) standard, which requires end-to-end acknowledgement for every message packet. If a message is not successfully delivered due to a network anomaly, the system automatically retries or alerts the telecommunicator.

- Foreign language translation for all texts; and descriptions of end-to-end text path measurement, translation delivery/display, monitoring for 99.99% availability, and logging/reporting procedures.

Motorola Response

Comply.

Foreign language translation is supported by the ability to conference language services into text or voice+text sessions, or directly on the call handling system, as enabled by the receiving PSAP.

TTY Translation, Delivery, and Display: The proposed Service supports the transcoding of Baudot tones to RTT. LNGs and LSRGs positioned near the network edge transcode Baudot tones and place the data into the media stream as early as possible; this process is engineered to minimize packet loss and audio issues. If a PSAP does not yet support RTT, the OSP will convert the RTT call to TTY until the PSAP is ready to accept native RTT.

Texts—including SMS, TTY, and RTT—are delivered through the NGCS and integrated directly with the PSAP CHE. The system uses the NGCS PRF to evaluate location data and route the texts to the appropriate destination over the ESInet. If text media is included within an emergency voice call, the PSAP will receive concurrent voice and text for the same wireless 9-1-1 call. Furthermore, the same circuit used to receive the SMS is utilized to deliver return messages from the PSAP back to the 9-1-1 caller.

End-to-End Text Path Measurement: To ensure complete transparency and measurement from call origination to termination, the solution relies on an end-to-end call tracking and reporting architecture. This integrates i3 logging, MIS data, and TCC reporting to track all elements of a text session across the NGCS, ESInet, TCCs, and the PSAP CHE. The system also includes extensive final acceptance and functional testing plans where Text-to-9-1-1 test calls are initiated to manually verify the text path. These tests evaluate delivery to the correct destination, bidirectional text functionality, and the overall accuracy of data sent and received.

Monitoring for 99.99% Availability: The provided system exceeds standard availability requirements by being engineered to achieve 99.999% operational availability (limiting downtime to no more than 5.26 minutes per year). To monitor and ensure this uptime, the system relies on the following processes:

- **24/7/365 NSOC Monitoring:** A dedicated NSOC provides continuous monitoring of the entire solution's performance and availability, covering all network, computing, and software elements, as well as OSP connections.
- **Dynamic Failover:** The architecture features geographically diverse data centers with quadruple-redundant FEs. The network utilizes dynamic routing protocols that provide rapid failure detection and automatic failover capabilities, automatically rerouting traffic to available paths during an incident to prevent service degradation.
- **Customer Visibility:** Real-time and near-real-time network node statuses, operational metrics, and SLA performances are visible to authorized personnel via a CWP.

Logging and Reporting Procedures: The solution offers a specialized Text-to-9-1-1 Reporting Suite that pulls data directly from the TCCs and integrates it with i3 Event Logging and CHE data for comprehensive analytics. Administrators can partition logs and schedule automated reports based on specific PSAPs or jurisdictions. Key text reporting procedures and capabilities include:

- **Session Transcript Reports:** Provides a complete line-by-line transcript for each text session, detailing start/end times, total duration, total messages, and the specific agent handling the call.
- **Volume Reporting:** Reports such as "Sessions Per Hour" and "Messages Per Hour" track the quantity of distinct text sessions and the volume of individual inbound/outbound messages across any given hour.
- **Performance Metrics:** Tracks call-taker performance using reports like "Agent Average Speed of Response" and "Initial Agent Speed of Answer," which gauge how quickly agents respond to incoming texts within defined timeframes.

2.4.3 Interactive Multimedia Response Service (IMRS)

The Respondent must provide a description and/or documentation that supports the requirements in this section, including IMR conforming to NENA-STA-010.3.

Motorola Response

Comply.

We comply with the NENA i3 (NENA-STA-010.3) standard for the Interactive Multimedia Response (IMR) functional element. Our IMR provides a native, standards-based mechanism for automated media interaction, queue management, and advanced call handling within the NGCS architecture.

- **Native i3 SIP & Media Negotiation:** Our IMR utilizes native SIP and Session Description Protocol (SDP) to establish and negotiate multimedia sessions. It strictly conforms to NENA-STA-010.3 requirements to ingest, process, and respond to multiple media types, including bidirectional audio, RTT, and standard SMS text via MSRP.
 - **Seamless ESRP & PRF Integration:** Positioned as a core i3 functional element, the IMR interfaces seamlessly with the ESRP. It executes complex PRF rules—such as playing standardized instructional announcements, managing interactive caller menus, or handling PSAP overflow queues—using standardized SIP call control.
 - **Standardized Header Preservation:** To ensure uninterrupted situational awareness, the IMR architecture natively parses, preserves, and appends mandatory NENA i3 SIP headers (including Call-Info, Geolocation, and History-Info). This ensures that critical location data and routing context are never stripped or lost during a caller's interaction with the IMR system.
 - **Accessibility & Multi-Modal Interactivity:** Conforming to NENA's strict accessibility guidelines, the IMR supports equitable, multi-modal interactions. It can intelligently provide dynamic, language-specific voice announcements or text-based interactive auto-replies, ensuring seamless communication for callers utilizing diverse or alternative communication methods.
-

2.4.4 Bridge

The State requires a multimedia bridge conforming to NENA-STA-010.3. The State expressly requires the bridge to handle audio, video, MSRP and RTT.

- The State has no preference on which model (ad hoc or answer all calls at a conference aware UA), but the bridge must be able to transfer calls to and from ESInets using either model as specified in NENA-STA-010.3.

Motorola Response

Comply.

-
- The bridge must have capacity to maintain 20 simultaneous 3-way video calls or 100 simultaneous 3-way audio calls or a mix thereof.

Motorola Response

Comply.

- The bridge must be capable of supporting up to 6 parties (caller, call taker and up to four other parties) in any conference, with any mix of media.

Motorola Response

Comply.

- The bridge must have a mechanism to support RTT mixing when the end points do not support multiple RTT streams conforming to RFC 9071, as specified in NENA-STA-010.3.

Motorola Response

Comply.

- The bridge must support logging of media using the NENA-STA-010.3 specified mechanisms.

Motorola Response

Comply.

- The bridge must support the RFC 4575 Conference Event Package.

Motorola Response

Comply.

- The bridge must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA 010.3. The State must be able to subscribe to ServiceState and receive the standard state changes. The proposal must describe the bridge in detail.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Multimedia bridge conforming to NENA-STA-010.3 handling audio/video/MSRP/RTT.

Motorola Response

Comply.

Our multimedia bridge is a native NGCS functional element that fully conforms to NENA-STA-010.3f. It is engineered to handle the simultaneous mixing of Audio, Video, MSRP (Instant Messaging), and RTT. By utilizing standard SIP signaling and RTP/RTCP media control, the bridge ensures that all participants in a conference—regardless of their device type—receive a high-quality, synchronized experience.

- Support for ad hoc or answer-all models with transfers using either.

Motorola Response

Comply.

Our bridge supports both Ad Hoc (user-initiated conferencing) and Answer-All (automated bridging) operational models. Telecommunicators can seamlessly initiate 3-way conferences or transfer calls using either model, ensuring that as a call is moved between PSAPs or extended to a secondary responder, the media continuity is preserved without requiring the caller to re-establish the session.

- Capacity for 20 simultaneous 3-way video or 100 audio calls (mix).

Motorola Response

Comply.

The bridge is architected for high-density public safety environments, supporting a baseline capacity that 30% of all calls will be conferenced. This approach is based on traffic forecasting and traffic management approach. We exceed the state's requirements listed below :

- 20 simultaneous 3-way video conferences.
 - 100 simultaneous audio calls.
 - A flexible mix of both, ensuring that massive multi-agency incidents do not exceed the core's bridging resources.
-

- Up to 6 parties per conference with media mix.

Motorola Response

Comply.

The bridge utilizes a redundant and highly available Media Service engineered to support up to 10 simultaneous conference endpoints in a single NGCS-based conference call. This 10-party limit is in addition to the initial 9-1-1 caller and the primary PSAP call taker

- RTT mixing per RFC 9071.

Motorola Response

Comply.

Our bridge natively implements RTT Mixing in accordance with RFC 9071 (RTP-Mixer Formatting of Multiparty Real-Time Text).

- Media logging per standard; RFC 4575 Conference Event Package.

Motorola Response

Comply.

In compliance with evidentiary standards, our bridge provides Media Logging of the mixed output as well as individual source streams. It natively implements the RFC 4575 Conference Event Package, allowing authorized logging services or PSAP consoles to "subscribe" to conference state changes. This ensures a complete audit trail of when parties joined, when they were muted, and when the conference was terminated.

- ElementState/ServiceState support.

Motorola Response

Comply.

The bridge provides 24/7 health telemetry through the **ElementState** and **ServiceState** framework. These states are reported to the NSOC, providing real-time visibility into bridge utilization and health. If bridge capacity reaches a pre-defined warning threshold (e.g., 80%), an alert is triggered, allowing the NSOC to dynamically scale resources or reroute traffic to redundant bridge instances.

- Detailed bridge description.

Motorola Response

Comply.

Motorola provides a carrier-grade Multimedia Bridge as a core functional element of the NGCS architecture, designed to orchestrate complex, multi-party emergency sessions. Unlike legacy audio bridges, this i3-compliant solution treats voice, video, and text as a unified session, ensuring all participants maintain full situational awareness.

- **Architectural Integration:** The bridge is a software-based functional element that resides within the geo-redundant ESInet core. It interfaces directly with the ESRP and uses standard SIP for call control. It is natively designed to handle "**Answer-All**" scenarios (where the bridge is pre-inserted into the call path) and "**Ad Hoc**" scenarios (where a dispatcher adds participants on the fly).

- **Standards-Based Signaling (RFC 4575):** The bridge implements the SIP Conference Event Package. This allows PSAP CHE to "subscribe" to the bridge for real-time updates. If a participant joins, leaves, or mutes their media, the bridge pushes a notification to the dispatcher's console, providing a visual roster of the active conference.
 - **Security and Trust:** In alignment with the "**Zero Trust**" model, every connection to the bridge is secured via Mutual TLS (mTLS). The bridge validates the digital certificates of all joining FEs against **PCA root**, ensuring that sensitive incident audio and data cannot be intercepted by unauthorized parties.
 - **Unified Media Mixing Engine:** The bridge utilizes a sophisticated mixing matrix that processes disparate media types simultaneously:
 - **Audio:** High quality mixing of G.711 and high-bandwidth codecs with automatic gain control and noise suppression.
 - **Video:** A "Switching" or "Selective Forwarding" mixer that delivers synchronized real-time video streams to all capable endpoints.
 - **MSRP/RTT:** A specialized text mixer that interleaves characters and messages chronologically, ensuring that the dispatcher sees a coherent thread from all parties.
-

2.5 Egress and External Interfaces

2.5.1 Outgoing Call Interface Function (OCIF)

The State requires an OCIF conforming to NENA-STA-010.3. The OCIF must be capable of directing a call back of an emergency call to the OSP that originated the emergency call, offering at least the same media streams negotiated in the emergency call. The contractor must obtain appropriate identities (for example, telephone numbers) for calls sent to other service providers. Use of those identities must be controlled by the Data Rights Management system specified in NENA-STA-010.3.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- OCIF per NENA-STA-010.3 for call backs to OSP with same media streams.

Motorola Response

Comply.

Motorola provides an OCIF that serves as the standardized gateway for all outbound traffic leaving the i3 PSAP. It is fully conformant with NENA-STA-010.3, functioning as a SIP Proxy/B2BUA to route callbacks, administrative calls, and inter-agency communications. Crucially, the OCIF ensures media parity; it is capable of initiating callbacks using the same media streams received in the original call—

including Audio, Video, MSRP (Text), and RTT—ensuring the dispatcher can re-establish the same level of situational awareness if a call is disconnected.

- Obtaining identities for other providers controlled by DRM.

Motorola Response

Comply.

The OCIF manages caller identity in accordance with the STIR/SHAKEN framework and NENA i3 security standards. When a dispatcher initiates a callback, the OCIF interacts with the Secure Telephone Identity – Authentication Service (**STI-AS**) to assert the PSAP's authoritative identity, ensuring the call is not blocked as spam by the recipient's carrier. Access to the identities of other service providers or specialized data repositories is strictly governed by **DRM** and **RBAC**, ensuring that sensitive provider information is only retrieved by authorized FEs for legitimate public safety purposes.

- Description of OCIF utilization for call backs with implementation/integration details.

Motorola Response

Comply.

The use of OCIF is natively integrated into the Motorola VESTA 9-1-1 and VESTA NXT call handling systems.

Automated Abandoned Callback (AAC): The OCIF supports our AAC feature, which automatically initiates return calls for abandoned 9-1-1 sessions. If the caller answers, they are immediately placed into the emergency queue; if they do not answer, the OCIF logs the attempt and can be configured to retry or alert a dispatcher.

Standardized Interfaces: The OCIF utilizes standard SIP/RTP interfaces to communicate with the ESInet core and external PSTN gateways. This integration allows for a seamless "one-click" callback experience from the dispatcher's map or call-handling interface, significantly reducing the response time required to re-engage with a citizen in distress.

3. GIS and Database Services Requirements

The Contractor shall implement location-based routing and ECRF/LVF functions using GIS data that conforms to the NENA GIS Data Model (NENA-STA-006.2), including civic address points, road centerlines, PSAP boundaries, emergency service polygons, and other required layers. The GIS repository must support spatial indexing for efficient queries.

Motorola Response

Comply.

Operations and Administration:

Location information is handled by the PSAPs while the State handles the PSAP boundaries and provisioning boundaries. The proposal shall include measures to maintain the PSAP interaction and where the PSAP utilizes a vendor must not interfere or materially change the contract a PSAP currently has for GIS support.

Motorola Response

Comply.

Location conveyance:

Location data shall be transported using PIDF-LO per RFC 4119 and RFC 5139 with applicable NENA extensions. The system shall deliver location information to PSAP CHE and mapping clients via standardized NG911 interfaces, supporting both push and pull mechanisms.

Motorola Response

Comply.

Validation and determination:

Integrate LVF/LIS to validate caller-provided locations, supporting geodetic coordinates (for example, WGS84) and civic addresses, including complex scenarios such as multi-line enterprises and multi-tenant buildings with address reformatting. The ECRF shall use authoritative GIS to determine the correct ESN/PSAP, with defined fallback to default routing.

Motorola Response

Comply.

Data governance and provisioning:

The GIS system shall provide change tracking, version control, time-stamped snapshots, and automated batch or incremental updates using NENA provisioning formats (for example, GML and GeoJSON). Provide a GIS data-provisioning API and a comprehensive audit log of changes, including user, timestamp, and deltas.

Motorola Response

Comply.

Rules-based routing (RBR):

Support RBR features, including time-of-day routing, temporary boundary adjustments, alternate routing logic, and attribute-driven decisions derived from GIS layers or an integrated rules engine.

Motorola Response

Comply.

3.1 Data Management and Interfaces

3.1.1 GIS and Database Management Functionality

The contractor will utilize the PSAP and State provided data for geospatial routing from the caller to the PSAP. Management of the data will be the responsibility of the State.

Motorola Response

Comply.

The contractor will have a web interface and/or automated method to provision data and retrieve post-QA data for the use of maps and/or the computer-aided dispatch (CAD) system. The contractor will ensure that an update to the system will be reflected in a change in routes (where the change does affect routes) within 5 minutes of such a change, assuming no errors are detected (online, real time update capability).

Motorola Response

Comply.

All data associated with call routing and plotting will be provided in conformance with NENA Data Model standards – NENA-STA-015.10 for remaining Legacy/Enhanced 911 systems and NENA-STA-006.2 for NG911 systems.

Motorola Response

Comply.

Originating call network operators will verify civic address location information against the NG911 GIS data using the LVF provisioned as required.

Motorola Response

Comply.

The preferred data exchange will be in Environmental System Research Institute's (ESRI) Structured Query Language (SQL) Spatial Database Engine (SDE).

Motorola Response

Comply.

The managed GIS map data will replace the traditional MSAG database as the primary database for location-based call routing and location validation (ECRF/LVF) functions within the NG911 system.

Motorola Response

Comply.

The maintenance of this GIS dataset will be completed by PSAP staff or designee. It is a requirement that the discrepancy reports of the data are delivered for remediation.

Motorola Response

Comply.

The contractor will be utilizing all existing and available source data and the management and coordination necessary.

- The PSAP will be responsible for providing all GIS data used in the location routing, validation, mapping services, and maintenance of such data that are part of the contractor's system.

Motorola Response

Comply.

- The data from the PSAP will include the road centerline and address range data, address structure points, PSAP boundaries, municipal boundaries, police, fire, EMS, and medical transport boundaries and many additional GIS layers useful for display in the PSAPs. GIS data used for call routing and call locations will be provided in a NENA NG911 standard format.

Motorola Response

Comply.

- The contractor will be required to establish a working relationship with the State and to work out mutually acceptable procedures for the maintenance of these databases.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Use of PSAP GIS data for geospatial routing.

Motorola Response

Comply.

Motorola NGCS utilizes the State's authoritative PSAP GIS data as the core logic for the ECRF. By performing spatial queries against address points, road centerlines and service boundaries, we ensure that every call is routed to the correct PSAP based on the caller's physical location, eliminating the errors associated with legacy tabular MSAG lookups.

- Web interface or automated method for provisioning and retrieving post-QA data for maps.

Motorola Response

Comply.

We provide a secure, web browser-based SI for the automated provisioning of GIS data. After GIS professionals perform local QA, data can be uploaded or synchronized automatically. The system processes this data, performs secondary validation, and distributes "routing-ready" datasets to the core maps and FEs without manual intervention. Critical and warning data errors are also available as features and reports for post-QA remediation.

- Reflection of PSAP updates in routes within 5 mins (online real-time).

Motorola Response

Comply.

Our architecture is designed for high-velocity updates. When a GIS change (e.g., a new street or boundary adjustment) is published via the SI, the update is reflected in the live ECRF/LVF routing tables within 5 minutes. This ensures that first responders and call-takers are always working with the most current jurisdictional information.

- Data structures organized in conformance to NENA Data Model Standards – NENA-STA-015.10 and NENA-STA-006.2.

Motorola Response

Comply.

All data structures within the Motorola LDB and ECRF/LVF conform to the NENA-STA-015.10 (Data Formats for E9-1-1 Data Exchange) and NENA-STA-006.2 (NG9-1-1 GIS Data Model) standards. This ensures that State of Nebraska's GIS layers including road centerlines, address points, and service boundaries are interoperable with national NG9-1-1 systems.

- LVF for OSP civic address verification.

Motorola Response

Comply.

We provide an i3-compliant LVF that allows OSPs and 9-1-1 authorities to pre-validate civic addresses against the local GIS database before a call is ever made. This proactive validation significantly reduces "Address Not Found" errors during emergency events.

- Preferred ESRI SQL SDE exchange.

Motorola Response

Comply.

Motorola prefers and supports direct ESRI SQL SDE (Spatial Database Engine) exchanges. This allows our systems to interface natively with the industry-standard ESRI ArcGIS environment, enabling efficient data replication, versioning, and high-performance spatial queries without the need for cumbersome file conversions.

- Replacement of MSAG with GIS for routing/validation.

Motorola Response

Comply.

Our solution facilitates the complete replacement of the legacy MSAG with GIS-based routing and validation. We provide tools to cross-validate existing MSAG records against GIS layers to identify and resolve discrepancies, ensuring a clean transition to a purely geospatial environment.

- PSAP maintenance with contractor discrepancy reports.

Motorola Response

Comply.

Maintenance: We provide full QA/QC on uploaded data with reports and feature extractions available to the 9-1-1 authority. We can also provide GIS Managed Services where our experts can perform all GIS data maintenance, including processing, publishing, and troubleshooting.

Discrepancy Reporting: Our system includes automated Discrepancy Reporting and Resolution (DRR) tools. When a routing or validation mismatch occurs, a report is generated for PSAP or contractor review.

- Use of existing source data.

Motorola Response

Comply.

Source Data: We utilize the State's and Counties' existing source data, protecting previous investments while enhancing them for NG9-1-1. We will accept uploads to the SI from the currently contracted GIS maintenance companies as well as those Counties that currently upload their data themselves.

- Responsibility for all GIS data maintenance.

Motorola Response

Comply.

Full-Service Data Stewardship: Motorola assumes full responsibility for the management of the GIS datasets powering the NGCS. Through our GIS Managed Services, a dedicated team of public safety GIS professionals handles the ongoing tasks of data ingestion, geo-processing, and synchronization. This "turnkey" approach means we take the labor-intensive responsibility for ensuring that road centerlines, address points, and jurisdictional boundaries are optimized for the ECRF and LVF.

Optimization and Standardization: Our experts perform the "nitty-gritty" work of data normalization—ensuring, for example, that varying street suffix abbreviations are standardized to prevent dispatch delays. We manage the transition from legacy tabular data (MSAG) to a purely spatial environment, taking responsibility for resolving the complex discrepancies that often arise during NG9-1-1 migration.

Quality Control and Accountability: While we assume responsibility for the technical maintenance, the State and local agencies retain full ownership and oversight of their data. We implement an automated Quality Control (QC) Plan that flags critical errors—such as polygon overlaps or gaps in PSAP boundaries—before they can impact live call routing. Discrepancies are tracked via a formal reporting process, ensuring every update is transparent and auditable.

- Inclusion of road centerline, address points, PSAP emergency boundaries, and additional layers.

Motorola Response

Comply.

Required Layers: We support and maintain all mandatory layers, including Road Centerlines, Site/Structure Address Points, PSAP Boundaries, and additional layers as mutually agreed upon.

- Mutually acceptable maintenance procedures with State.

Motorola Response

Comply.

Motorola will collaborate with the State to establish Mutually Acceptable Maintenance procedures. This includes defined sync schedules, escalation paths for data errors, and clear roles for local vs. contractor data updates.

3.1.2 Spatial Interface (SI) Functionality

The contractor will implement a Spatial Interface and ensure following capabilities are implemented:

- GIS data provisioned by the spatial interface (SI) will undergo data-quality and data-integrity checks to ensure that the data complies with all applicable requirements of NENA-STA-015.10-2018, NENA-STA-006.2-2022, NENA-02-014 and NENA-STA-010.3-2021 while maintaining the online, real time update capability.

Motorola Response

Comply.

- The SI will convert the GIS data meeting these requirements into the format (data structure and projection) used by the ECRF and LVF, in real-time or near-real-time, using a Web feature service.

Motorola Response

Comply.

- The SI will be able to provision and perform incremental updates, in near-real-time, to the ECRF, LVF, the map viewer service, the PSAP map display and similar applications that consume GIS data.

Motorola Response

Comply.

- Validation of GIS data and data updates prior to their provisioning into the ECRF and LVF, along with the means of online real-time provisioning of updates to the GIS data provisioned to the ECRF and LVF.

Motorola Response

Comply.

- The SI operation will align with the data maintenance processes with minimal impact to existing operations.

Motorola Response

Comply.

- The SI will receive and incorporate the SI datasets that have been prepared by the PSAP as previously described.

Motorola Response

Comply.

- Web interface tool for viewing and submitting incidents and change tickets.

Motorola Response

Comply.

- Web interface tool for viewing policy-routing plans.

Motorola Response

Comply.

The contractor will be able to test and then apply updates to the operating ECRF by a secure and reliable method that does not create operational problems.

Motorola Response

Comply.

The contractor's GIS functions will be able to perform database audits for common problems and errors, such as gaps, overlaps or number range conflicts, which if encountered, will be referred back to the PSAP for resolution.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SI implementation with data-quality and integrity checks per NENA standards while maintaining real-time updates.

Motorola Response

Comply.

The Motorola SI uses a strong validation engine to check schema, attribute, domain, and geometry to meet and exceed the NENA standards. It can issue warnings for failed validations, allowing the data to proceed, or errors that block data uploads from moving to systems like the ECRF and LVF.

- Conversion to ECRF/LVF format via Web feature service.

Motorola Response

Comply.

The SI can integrate with a customer's data maintenance environment by consuming Web Feature Services (WFS). It processes the data like any other GIS upload, performing quality checks to ensure accuracy and consistency before sending it to the LVF and ECRF.

- Incremental near real-time updates to ECRF/LVF, map viewer, and PSAP displays.

Motorola Response

Comply.

The SI supports incremental updates to support accurate and timely updates to downstream systems (e.g. ECRF/LVF, map viewer, and PSAP displays).

- Validation prior to provisioning with online real-time updates.

Motorola Response

Comply.

The SI provides a validation engine for all data updates that flow through the system to ensure data accuracy and consistency prior to sending the data to downstream systems.

- Alignment with PSAP processes.

Motorola Response

Comply.

Motorola will work with the PSAPs, State and contracted maintenance providers to ensure agreed upon processes are in place.

- Incorporation of PSAP prepared datasets.

Motorola Response

Comply.

Motorola's SI can consume a number of different data formats including the NENA NG9-1-1 GIS data model.

- Web tools for incidents, change tickets and policy-routing views

Motorola Response

Comply.

Motorola provides web interface tools for viewing and submitting incidents and change tickets primarily through two interconnected platforms: the **CWP** and the **Customer Hub**. These platforms are integrated with Motorola's IT Service Management (ITSM) tool, ServiceNow, to provide a centralized and transparent view of support activities.

The CWP The CWP is a secure, web-based interface that provides comprehensive, permissions-based visibility into the technical health and operations of the NG9-1-1 service. Key features related to incidents and changes include:

- **Case Management Module:** Authorized users can access this persona-based module to view and manage both trouble tickets and Change Management activities across the entire solution, all in a single view.
- **Real-Time Dashboarding:** The portal uses maps, graphs, and tables to present near real-time details on critical FEs, network health, and active routing exceptions.

- **Event Tracking and Escalations:** It features dedicated tabs for alerts and notifications, allowing users to efficiently track active incidents, understand planned maintenance events, review historical service cases, and access escalation points and procedures for easy reference.

The **Customer Hub** serves as the specific user interface into Motorola's support structure, acting as the direct front-end for the ServiceNow ticketing system. Key capabilities include:

- **Shared Information:** It provides users with direct access to the same incident management information and case details utilized by Motorola's engineers and managers.
- **Ticket Submission and Tracking:** Users can create new low-priority cases or service requests, add updates, or modify existing tickets.
- **Change Event Visibility:** The Hub allows users to view the real-time status of scheduled activities, such as change authorization requests, service requests, and application security patches.

Important Usage Constraint While the CWP and Customer Hub are highly effective for tracking information and submitting routine items, Motorola explicitly notes that these web portals are not monitored for an instantaneous response. Therefore, **all Critical and High-priority incidents must be reported via their 24/7 toll-free telephone number** rather than through the web interfaces to ensure immediate troubleshooting and response.

- Secure reliable update and testing application without problems.

Motorola Response

Comply.

The SI is a secure web interface that allows for test data to flow through the system to verify system integrity.

- Database audits for gaps/overlaps/conflicts referred to PSAP

Motorola Response

Comply.

The SI supports Gap and Overlap validations to ensure data quality. The data can then be downloaded by authenticated users for dissemination and error resolution.

3.2 Core Data Services

3.2.1 Mapping Data Service

A Mapping Data Service conforming to NENA-STA-010.3 will be provided. This must be available within 18 months. The MDS will be capable of providing maps for all calls for all entities inside the ESInet and for calls handled out of area in other ESInets.

- The MDS must support both images and features as described in NENA-STA-010.3

Motorola Response

Comply.

- The MDS must support all layers defined in NENA-STA-006.2. Additional layers may be supported, and the proposal will describe what additional layers the MDS will support.

Motorola Response

Comply.

- Retrieval of map data must be controlled by the NENA-STA-010.3 Data Rights Management mechanism.

Motorola Response

Comply.

- The MDS must support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3. The State must be able to subscribe to ServiceState and receive the standard state changes.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- MDS per NENA-STA-010.3 available within 18 months for all calls/entities.

Motorola Response

Comply.

We are committed to providing the MDS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

-
- Support for images/features.

Motorola Response

Comply.

We are committed to providing the MDS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

- All layers per NENA-STA-006.2.

Motorola Response

Comply.

We are committed to providing the MDS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

- Additional layers described; DRM-controlled retrieval; ElementState/ServiceState support with State subscription.

Motorola Response

Comply.

We are committed to providing the MDS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

3.2.2 MSAG Conversion Service (MCS)

The MSAG Conversion Service (MCS) shall support the standard SI interface for provisioning. The proposal may include additional options that would lessen the burden on PSAPs upgrading their GIS systems to NG standards.

Motorola Response

Comply.

The State expects the LNG to support the SOA interface towards the legacy OSP, store the data in the Location Database in LVF-valid form and convert it to and from the legacy data formats using the MCS.

Motorola Response

Comply.

The State expects the LPG to support the MF/ALI interface towards the legacy PSAP, retrieve the location from a Location Information Server in LVF-valid form and convert it to and from the legacy data formats using the MCS.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An MSAG Conversion Service (MCS) conforming to NENA-STA-010.3 will be implemented.

Motorola Response

Comply.

Motorola will provide a NENA-STA-010.3 compliant MCS.

- The MCS must support Element State and Service State SUBSCRIBE/NOTIFY per NENA-STA 010.3.

Motorola Response

Comply.

The MCS supports both ElementState and ServiceState as defined by NENA-STA-010.3.

- The State must be able to subscribe to Service State and receive the standard state changes.

Motorola Response

Comply.

Motorola will support the State subscribing to MCS ServiceState notifications.

3.2.3 Geocode Conversion Service (GCS)

The Geocode Conversion Service (GCS) shall support the standard SI interface for provisioning. The proposal may include additional options that would lessen the burden on PSAPs upgrading their GIS systems to NG standards.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- GCS per NENA-STA-010.3 with SI provisioning (additional options for PSAP GIS upgrades).

Motorola Response

Comply.

We are committed to providing the GCS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

- Return of ECRF routing location for civic addresses.

Motorola Response

Comply.

We are committed to providing the GCS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

- ElementState/ServiceState support.

Motorola Response

Comply.

We are committed to providing the GCS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

- ServiceState and receive the standard state changes.

Motorola Response

Comply.

We are committed to providing the GCS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

- The GCS must return the same location that the ECRF uses for routing when given a civic address.

Motorola Response

Comply.

We are committed to providing the GCS and will work with the State to determine a timeline for implementation and have this available upon agreement between all parties.

3.3 PSAP-Facing Services

3.3.1 PSAP Mapping Service

The State requires a Mapping Data Service (MDS) conforming to NENA-STA-010.3.

Motorola Response

Comply.

The services required must enable the PSAP mapping system and ECRF/LVF system to support multiple methods for reporting location errors. They include:

- ECRF civic location geocoding errors are automatically captured by the data management application utilized by the PSAP.

Motorola Response

Comply.

- LVF failures are automatically captured by the LVF and forwarded to the data management application utilized by the PSAP.

Motorola Response

Comply.

- 911 call mapping failures (calls that could not be mapped automatically) are captured by the system and forwarded to the data management application utilized by the PSAP.

Motorola Response

Comply.

- 911 telecommunicators and dispatchers may manually generate a discrepancy report, and the system can automatically forward the reports to the data management application utilized by the PSAP.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- PSAP mapping using PSAP geospatial info.

Motorola Response

Comply.

The SI can support the needs of the PSAP's mapping system by formatting the uploaded data to conform to the mapping system's data schema.

- Support for error reporting methods (ECRF geocoding errors captured).

Motorola Response

Comply.

Motorola staff will run reports, research the errors returned by the ECRF, and assist with their remediation.

- LVF failures forwarded; unmapped calls captured; manual discrepancy reports forwarded.

Motorola Response

Comply.

Motorola's LoST service captures failed LVF and ECRF queries for error resolution. Discrepancies can be created manually and submitted to the appropriate team for error resolution.

3.3.2 Map Discrepancy Reporting

The Respondent must provide a description and/or documentation that supports the requirements in this section for referral of all geospatial discrepancies to the State for remediation.

Note:

GIS-related discrepancy reporting technical requirements are detailed in §E-6.7.2, et seq. of this document.

Motorola Response

Comply.

Motorola will provide a report of all map/GIS based discrepancies to the State of Nebraska for error resolution. The reports will include ECRF, LVF and MCS query failures due to mismatches in the GIS data.

3.4 External Integrations

The Respondent must provide a description and/or documentation that supports the integration with additional vendors as required to provide functionality to all PSAPs as currently utilized.

Motorola Response

Comply.

Motorola continually conducts structured interoperability testing with third-party ECH providers to ensure compatibility, reliability, and standards compliance. Testing validates call setup, signaling, media exchange, location data handling, and security across interfaces using defined test plans and success criteria.

Tests are performed in controlled lab and production-like environments, with results documented and issues tracked to resolution. Regression testing is conducted after upgrades or configuration changes. Detailed reports capture test scope, outcomes, defects, and corrective actions to confirm ongoing interoperability.

The following table lists the call handling systems which have completed IOT with the VESTA NXT Router Services or currently testing.

Table 5-1: External Integration

PSAP Controllers	Status
Motorola VESTA 9-1-1 R8.3 HF1	IOT certified and interconnected with Motorola NGCS
Motorola VESTA NXT	IOT certified and interconnected with Motorola NGCS
Motorola CallWorks 4.4.7	IOT certified and interconnected with Motorola NGCS
Solacom Guardian	IOT Certification process has been initiated
Intrado Viper 7.0 SP3	IOT Certified and interconnected with Motorola NGCS
Carbyne APEX	IOT Certified
CentralSquare	IOT testing in process

4. Security Requirements

The contractor shall implement the NENA NG-SEC security and trust model, featuring strong authentication and authorization for all interfaces, mutual TLS for inter-service communications, edge security via SBCs and Back-to-Back User Agents (B2BUAs), network segmentation, and secure management planes. Threat mitigations must address Denial of Service (DoS), Distributed DoS (DDoS), Telephony Denial of Service (TDoS), SIP flooding, spoofing, and injection attacks through rate limiting, anomaly detection, and firewalls.

Motorola Response

Comply.

Implement Role-Based Access Control (RBAC) with granular permissions, multifactor authentication (MFA) for all administrative access, least privilege enforcement, and auditing of service accounts. Integration with external identity providers (e.g., SAML/OAuth) must be supported.

Motorola Response

Comply.

All location data, call content, and PII must be encrypted in transit (TLS 1.3) and at rest (AES-256 or stronger), with data minimization, pseudonymization, and compliance with laws like HIPAA and CJIS where applicable. Access to sensitive data shall require explicit consent logging.

Motorola Response

Comply.

Provide Public Key Infrastructure (PKI) processes for certificate issuance/rotation, Certificate Revocation List (CRL)/Online Certificate Status Protocol (OCSP) validation, and secure key storage using Hardware Security Modules (HSMs) or compliant vaults. Automated alerts for expiring certificates must be included.

Motorola Response

Comply.

The contractor shall supply an incident response plan aligned with NENA, including vulnerability disclosure protocols, regular patch schedules (e.g., critical patches within 30 days), and forwarding of security event logs to the jurisdiction's Security Information and Event Management (SIEM) system via secure channels (e.g., Syslog over TLS).

Motorola Response

Comply.

Provide results from independent penetration testing (conducted within the last 12 months), SSAE 18/SOC 2 audit reports, and support for jurisdiction-led security acceptance testing, including network scans, application fuzzing, and red-team exercises.

Motorola Response

Comply.

4.1 Management and Process Control

4.1.1 Personnel Roles and Responsibilities

Safeguarding NG911 assets – across NGCS platforms and the ESInet – is a shared duty. The contractor must define, assign, and document minimum security roles and responsibilities, whether performed internally or by external providers. At a minimum, the following roles must be covered by named, accountable individuals. Where third parties perform duties (carriers, cloud, managed services, subcontractors), the contractor remains responsible for assignment and verification.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An organizational roles matrix (e.g., org chart and/or RACI) identifying named individuals (or positions) for: Security Manager, Security Administrator, Data Owner(s), Data Custodian(s), Data User populations, and Security Audit Manager. Note any shared/combined roles and the accountable individual for each responsibility. Map these to NGCS components and ESInet segments.

Motorola Response

Comply.

While Motorola maintains an extensive internal library of cybersecurity and Governance, Risk, and Compliance (GRC) documentation detailing these role definitions and policy authorities, these internal documents are not released publicly. Instead, the enforcement of these controls and authorities is validated by independent third-party audits, including our ISO 27001:2022 certification and SSAE 18, SOC 2, Type 2 reports (which cover Security, Availability, Processing Integrity, Confidentiality, and Privacy).

- Documented role definitions aligned to the duties above, including authorities (e.g., the Security Manager's authority to set security policy for all NGCS/ESInet components; Security Administrator authority to implement and enforce controls across applications, network, cloud).

Motorola Response

Comply.

Motorola enforces hardened physical and virtual access control policies and oversight to ensure that users are strictly limited to performing actions and accessing system elements that are explicitly required by their specific roles, responsibilities, rights, and permissions. NENA NG-SEC compliance standards dictate that personnel performing security or entity administration ensure that only approved entities are granted access, and that requests for user authorizations are documented.

While Motorola maintains an extensive internal library of cybersecurity and Governance, Risk, and Compliance (GRC) documentation detailing these role definitions and policy authorities, these internal documents are not released publicly. Instead, the enforcement of these controls and authorities is validated by independent third-party audits, including our ISO 27001:2022 certification and SSAE 18, SOC 2, Type 2 reports (which cover Security, Availability, Processing Integrity, Confidentiality, and Privacy).

- Evidence that personnel are informed of their roles and responsibilities (e.g., acknowledgement forms, training records, onboarding materials, policy attestations).

Motorola Response

Comply.

Evidence of personnel awareness is embedded in our stringent onboarding and continuous education practices. All personnel undergo background checks prior to employment and are required to participate in periodic cybersecurity awareness training courses as well as other ongoing awareness exercises. Additionally, our dedicated cybersecurity personnel receive formal security training and maintain relevant industry certifications from recognized authorities such as SANS, (ISC)2, and ISACA.

Compliance with these personnel training requirements, policy attestations, and role definitions is regularly audited as part of our ISO 9001-2015 certification and SOC 2 Type 2 reporting. To ensure personnel responsibilities align with system access, we also conduct a quarterly review (true-up) of all physical and logical access control lists (ACL) to confirm that only current employees with a verified business need retain access to NGCS and ESInet components.

-
- A data ownership register mapping every NG911 data set (local and remote) to a Data Owner; include classification and handling responsibilities.

Motorola Response

Comply.

We maintain a master register mapping all NG9-1-1 datasets (GIS layers, CDRs, EIDOs) to their respective Data Owners. This register includes classification levels (e.g., Sensitive/Public Safety) and detailed handling instructions to prevent unauthorized disclosure or modification.

-
- A data custodianship register mapping every NG911 data set (at rest and in transit, local and remote) to a Data Custodian; include the operational security measures they manage (encryption, key management touchpoints, access administration, backup/restore).

Motorola Response

Comply.

The register identifies the Data Custodian for every dataset at rest and in transit. It outlines managed operational security measures, including:

- **Encryption:** AES-256 for data at rest; TLS 1.2+ for data in transit.
- **Key Management:** Defined touchpoints for HSM or cloud-based key rotations.
- **Availability:** Backup/restore procedures and RTO/RPO (Recovery Time/Point Objectives).

-
- Security administration procedures showing how the Security Administrator implements and maintains security controls in accordance with NG911 policies – for NGCS applications, the ESInet, edge devices, and management portals).

Motorola Response

Comply.

The register identifies the Data Custodian for every dataset at rest and in transit. It outlines managed operational security controls, including:

- **Encryption:** AES-256 for data at rest; TLS 1.2+ for data in transit.
 - **Key Management:** Defined touchpoints for HSM or cloud-based key rotations.
 - **Availability:** Backup/restore procedures and RTO/RPO (Recovery Time/Point Objectives).
-

- An audit governance plan for the Security Audit Manager covering periodic audit cadence (internal/external), scope, reporting, and risk rating of findings, and tracking to closure.

Motorola Response

Comply.

The Security Audit Manager follows a defined audit cadence. This includes:

- Quarterly Internal Audits: Focusing on access logs and configuration drift.
 - Annual External Audits: Conducted by independent third parties (e.g., SOC2, FedRAMP).
 - Risk Mitigation: Findings are assigned a risk rating (Critical to Low) and tracked to closure through a formal Remediation Plan.
-

- Role coverage procedures (e.g., delegation during absence) ensuring continuity while preserving single-point accountability for each required responsibility.

Motorola Response

Comply.

To guarantee continuous operational capability throughout the year, we establish Delegation of Authority protocols. In the event of absences, duties are officially transferred to a designated individual, who is appointed and involved as necessary to ensure uninterrupted coverage and continuity. This procedure guarantees that while "single-point accountability" is maintained, there is never a gap in security supervision or administrative authority.

- If external parties are involved, contractual or policy evidence assigning role responsibilities to vendors/contractors/subcontractors and showing how the prime provider verifies fulfillment (e.g., attestations, SLAs, right-to-audit).

Motorola Response

Comply.

Where subcontractors or third-party OSPs are involved, our contracts include specific Security Flow-Down clauses. We verify fulfillment through annual attestations, specific SLAs for security incident response, and a clear right-to-audit clause, allowing the State to verify that all vendors meet the Nebraska NG9-1-1 security mandate.

Note: No subcontractors or consultants are anticipated for the execution of this project.

4.1.2 Identity Management

The contractor must operate a standards-based Public Key Infrastructure (PKI) to uniquely identify and authenticate every participating agency and agent across all NGCS and ESInet interfaces. An agency's identity must be a globally unique FQDN (e.g., `erie.psap.ny.us`) encoded in the X.509 `SubjectAltName` (SAN). An agent's identity must use the `user@agencyfqdn` format (e.g., `nancy@erie.psap.ny.us`) and be encoded in the SAN of the agent certificate.

Motorola Response

Comply.

- For PSAPs and 911 Authorities, the **PSAP Credentialing Agency (PCA)** is the **root of trust** for agency and agent certificates. The trust chain may include **national** → **state** → **agency/PSAP CAs**. Issuance may be performed directly by the PCA or by approved subordinate CAs under that chain. Any issuing authority must operate under a formal **Certificate Policy/Certification Practice Statement (CP/CPS)** with documented identity proofing and issuance controls. If an agency cannot meet those controls, it must use a **managed CA** that enforces the CP/CPS.

Motorola Response

Comply.

Private keys must be safeguarded in FIPS 140-2 validated cryptographic modules at these minimum levels: Level 2 for agency private keys (Level 3 preferred), Level 3 for agency CA keys, and Level 4 for state/national CA keys. Certificate-based authentication (e.g., mTLS) must be enforced so that valid identities and credentials are required for access to all NGCS/ESInet services and data (e.g., SIP signaling, APIs, management portals, interconnects).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An identity and certificate schema showing agency FQDN conventions and agent identifier format (`user@agencyfqdn`), with confirmation these identifiers appear in X.509 SAN fields for agency and agent certificates.

Motorola Response

Comply.

Identity and Certificate Schema Motorola utilizes a standardized Fully Qualified Domain Name (GQDN) convention for all agencies and agents.

- Agency FQDN: agencyname.nebraska.gov (e.g., lancaster-psap.nebraska.gov).
 - Agent Identifier: user@agencyfqdn (e.g., jsmith@lancaster-psap.nebraska.gov).
 - X.509 Verification: We confirm that these identifiers are populated in the Subject Alternative Name (SAN) field of the respective certificates. Agency certificates include the FQDN in the DNS Name SAN field, while Agent certificates include the Agent ID in the rfc822Name or another appropriate SAN field.
-

- A PCA/PKI trust architecture (diagram & narrative) showing the PCA root, any national → state → agency CA tiers, and permitted subordinate issuing models (e.g., PSAP/Authority issuing agent certs).

Motorola Response

Comply.

Our architecture adheres to the NIOC guidelines for the PCA.

- **National Root:** The National PCA Root anchors the trust for all NG9-1-1 entities in the United States.
 - **State/Regional CA:** Motorola acts as the regional PCA and operates its own ICA utilizing RSA 2048-based certificates. The system is designed to integrate with the NIOC PCA once fully established.
 - **Agency CA:** Motorola obtains and maintains the certificates technically required for the NGCS)interconnections to the PSAPs. All system components and FEs carry valid identity certificates that are traceable to a public source of trust, Motorola's ICA, and the National PCA (when available).
 - **Issuing Models:** We support decentralized issuing where the PSAP/Authority issues Agent certificates, ensuring that local administrative control is maintained within the global chain of trust.
-

- A current CP/CPS (or binding reference) for each issuing authority, defining identity proofing, issuance, renewal, revocation, auditing, and key management; state who operates each CA (Respondent, State, third party) and how compliance is enforced.

Motorola Response

Comply.

We commit to providing the required Certificate Policy/Certification Practice Statement (CP/CPS), or binding reference, for each issuing authority as part of our initial and ongoing contractual deliverables if awarded the contract.

The following exhibits provide the additional reference material requested:

Exhibit 7 - NIOC-PCA-Validation-Policy-v1.0-02-09-2022.pdf

Exhibit 8 - NIOC-PSAP-Credentialing-Agency-PCA-Certificate-Policy-v1.2-06-26-2024.pdf

- Key protection evidence demonstrating FIPS 140-2 validation and deployment at required levels:
 - Agency private keys: Level 2 minimum (note if Level 3 is implemented).
 - Agency CA keys: Level 3
 - State/National CA keys: Level 4

Motorola Response

Comply.

FIPS 140-2 Key Protection Evidence All cryptographic operations and key storage are performed on FIPS 140-2 validated modules:

- Agency Private Keys: Protected at Level 2 minimum (often Level 3 via hardware tokens).
 - Agency CA Keys: Stored in HSMs validated at Level 3.
 - State/National CA Keys: Stored in air-gapped or high-security HSMs validated at Level 4.
 - Evidence: We maintain a detailed device inventory and provide validation certificates for each HSM/token. All master CA keys are hosted in Tier-3 or Tier-4 data centers with strict escrow and DR arrangements.
-

- Key protection evidence should include device inventories, validation certificates, hosting locations, and any escrow arrangements.

Motorola Response

Comply.

Device Inventories: While the sources do not explicitly name a standalone "cryptographic device inventory," the provider is required to supply comprehensive hardware and software inventories. Upon system implementation and prior to final acceptance, Motorola provides detailed "as-built" documentation, network diagrams, and comprehensive equipment lists. This documentation clearly identifies all applications, appliances, and FEs deployed within the NG9-1-1 system.

Validation Certificates: The proposed solution strictly adheres to NIST FIPS 140-2 and FIPS 140-3 security requirements for cryptographic modules. As evidence of their broader security posture and controls, Motorola undergoes independent, third-party security audits. They provide Service Organization Controls (SSAE 18, SOC 1 Type 2, and SOC 2 Type 2) reports, which cover security, processing integrity, and confidentiality, as well as proof of ISO 27001:2022 and ISO 9001:2015 certifications. Note: Because Motorola's detailed Governance, Risk, and Compliance (GRC) documentation is proprietary, you must execute a Non-Disclosure Agreement (NDA) or access letter to review the full audit reports and validation certificates.

Hosting Locations: Key systems and FEs are hosted in a highly secure, geographically diverse architecture:

- The NGCS are deployed in a multi-cloud native architecture across a minimum of three geographically diverse cloud regions (utilizing multiple providers like AWS and Azure) with multiple Availability Zones.
- Physical data center facilities utilized for hosting elements meet a minimum of Tier 3 (Thermal Rejection) and Tier 4 (Power) availability and operational controls.
- The exact physical and logical locations, along with the configuration of each NGCS functional element, are meticulously detailed in the final "as-built" diagrams provided to the agency.

Escrow Arrangements: The provided sources do not contain any information regarding key escrow or software escrow arrangements as part of their security or cryptographic key protection strategy. (The only mention of "escrow" in the documentation relates to a third-party financial escrow account established for royalty payments stemming from unrelated corporate litigation). You may need to directly request information from the vendor regarding their specific escrow policies for cryptographic keys.

- Access control enforcement description confirming certificate-based authentication (e.g., mTLS) is required for all NGCS/ESInet services and data, where enforcement occurs (interfaces, APIs, signaling paths), and how failed, expired, or revoked certificates are detected and blocked.

Motorola Response

Comply.

Our proposed solution mandates certificate-based authentication to secure services and data. For SIP messaging, the system utilizes SIPS (SIP over a TLS-encrypted channel) and specifically mandates the use of Mutual Authentication (mTLS). All digital certificates used for this authentication must be CA-signed, issued either by the PCA or an authorized third-party Certificate Authority (CA).

- Certificate profiles and samples (agency and agent): SAN contents, Key Usage/EKU, validity periods, revocation mechanisms (CRL/OCSP), and sample chains validating to the PCA.

Motorola Response

Comply.

The following is a sample certificate chain from an existing Motorola NGCS deployment which is leveraging a PCA as its root of trust.

Device certificate:

Common Name: ecrfab.ng911.telus.ca

Subject Alternative Names: ecrfab.ng911.telus.ca, ecrf.ng911.telus.ca, IP Address: 75.156.201.19,
othername:elementId/ecrfab.ng911.telus.ca/ECRF/ng911.telus.ca

Organization: TELUS Communications Inc.

Organization Unit: ECRF Alberta

Locality: Vancouver

State: British Columbia

Country: CA

Valid From: February 20, 2024

Valid To: March 17, 2026

Issuer: TELUS ICA2, TELUS Corporation

Serial Number: 2c0c9a37a3216966043fa9e1b6cd7b7d7fb0d1ee

Intermediate certificate:

Common Name: TELUS ICA2

Subject Alternative Names: othername:<unsupported>

Organization: TELUS Corporation

Organization Unit: ICA2-0001

Locality: Vancouver

State: British Columbia

Country: CA

Valid From: March 15, 2022

Valid To: March 15, 2032

Issuer: TELUS CPCA Root CA, TELUS Corporation

Serial Number: 51930561626244 (0x2f3b06adc084)

Root certificate:

Common Name: TELUS CPCA Root CA

Subject Alternative Names: othername:<unsupported>

Organization: TELUS Corporation

Organization Unit: Root CA-1

Locality:

State:

Country: CA

Valid From: March 15, 2022

Valid To: March 15, 2042

Issuer: TELUS CPCA Root CA, TELUS Corporation

Serial Number: 3917653946751 (0x390265f317f)

- Operational lifecycle procedures for issuance, renewal, suspension/revocation, replacement, and compromise response; include joiner/mover/leaver workflows for agents and rollover plans for CA keys.

Motorola Response

Comply.

We maintain documented operational lifecycle procedures covering certificate issuance, renewal, suspension, revocation, replacement, and incident response for key compromise. Controls include identity verification, approval workflows, automated renewal, revocation of risk events, secure key storage, logging, and defined response steps for suspected or confirmed compromise.

Joiner, mover, and leaver workflows are enforced for all agents. Access and certificates are issued on onboarding, updated on role changes, and immediately revoked on termination. CA key rollover plans are defined and tested, including scheduled rotations, emergency rollover procedures, cross-signing where required, and communication plans to minimize service impact.

The system employs strict role-based access controls and principle of least privilege, supported by documented procedures for personnel lifecycle events:

Joiner / Mover / Leaver (JML) Workflows.

- **Joiners (New Users):** All requests for new user accounts, User IDs, and file/resource authorizations must be formally documented. Personnel performing security administration must ensure that only approved entities are granted access. All personnel undergo background checks before employment.
- **Movers (Role Changes):** The organization maintains formal procedures for changing access authority when an employee's role changes. Employees are prohibited from sharing private encryption keys except when appropriate authorities demand the key be surrendered due to a promotion or role change.
- **Leavers (Terminations):** There are strict procedures for immediately removing access authority for terminated personnel. If an employee is terminated, they are required to surrender any encryption keys for which they are responsible.
- **Auditing/True-ups:** To ensure these workflows are enforced, ACLs are maintained, updated as needed, and subjected to a mandatory quarterly review (true-up) to verify that only current personnel with a valid business need retain access.

Revocation and Compromise Response

- **Mandatory Reporting:** Key holders are required by policy to initiate key revocation if they believe access to their keys has been compromised.
- **Revocation Mechanisms:** A formal revocation procedure is in place for compromised digital certificates. The system actively checks the CRL for the specific certificate type to ensure the credential has not been revoked before permitting access.
- **Compromise Incident Response:** If a compromise occurs, it falls under the broader Incident Management Policy. The response process includes containing the attack to prevent further damage, eradicating the malicious code/actor, restoring affected systems to full functionality, and conducting a post-incident analysis to identify root causes and implement preventative measures.

Issuance, Renewal, and CA Key Rollover

- **Issuance and Renewal:** While the exact technical steps are kept internal, the security policy dictates that digital certificates must be kept current. Expired or invalid certificates are strictly prohibited from use, and the system verifies that the date the certificate is being used falls within its validity period.
 - **CA Key Rollover Plans:** The provided documentation does not explicitly detail the rollover plans or rotation schedules for CA keys. Because Motorola does not publicly release its internal Governance, Risk, and Compliance (GRC) manuals, specific details regarding CA key ceremonies and rollover contingencies would need to be reviewed under a Non-Disclosure Agreement via their SOC 2 Type 2 or ISO 27001 audit reports.
-

- Contingency approach if an entity cannot securely operate a CA (e.g., use of a managed CA aligned to the CP/CPS), including contractual controls, SLAs/SLOs, and audit rights.

Motorola Response

Comply.

Our proposed solution fully supports the contingency approach for entities unable to securely operate their own Certificate Authority (CA) by providing a managed CA service model.

Managed CA Approach (Contingency): If a local entity or state cannot securely operate its own CA, Motorola assumes this responsibility as part of its managed NGCS offering. Until a state or national authority is fully established, Motorola acts as the PCA and operates its own ICA utilizing RSA 2048-based certificates.

4.1.2.1 Roles

Every **agency** and **agent** must authenticate with an X.509 certificate that asserts one or more roles used for authorization.

Motorola Response

Comply.

- **Agency roles** define organizational authority, optionally constrained by **scope**.

Motorola Response

Comply.

- **Agent roles** define individual privileges and may include **modifiers** as identified in NENA-STA-010.3§5.3.

Motorola Response

Comply.

Role assignment for any agency or agent must be **approved and limited by the immediately superior agency's policy**. Solutions may support local roles, but **full functionality must work with baseline roles and scopes** for mutual aid and roaming. Roles must be **encoded in certificates** (role OIDs/attributes per profile) and **enforced at NGCS/ESInet interfaces**.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A role model and governance describing agency role, agent roles, and allowed scopes, including how the immediately superior agency approves/limits assignments and how those policies are enforced.

Motorola Response

Comply.

Motorola operates under a governance model where it serves in an advisory and operational support role, while the procuring agency (e.g., a state 9-1-1 board, county, or Emergency Communications District) acts as the central authority. The local agency retains control over operational workflows and is responsible for defining the PRR that govern how emergency calls are handled.

The immediately superior agency governs assignments by approving role and scope combinations before issuance. Enforcement occurs at credential issuance and at authentication: certificates or tokens are issued only if assignments match policy, and relying systems validate that presented roles and scopes are permitted by the governing agency policy. Any role or scope not explicitly approved is rejected.

- Role encoding specification for X.509 showing exactly how roles/modifiers/scopes are carried (e.g., OIDs or SAN/subject attributes) with minimal sample certs limited to the role fields and a description of validation during authentication.

Motorola Response

Comply.

Roles are carried as custom OIDs in the Subject or in an extension (preferred), scopes as SAN entries (e.g., otherName with a registered OID), and modifiers as additional OID-value pairs. Sample certificates are minimal and only display the relevant fields, for example:

X509v3 extensions: 1.2.3.4.1 = role:admin, 1.2.3.4.2 = scope:payments.read or SAN:
otherName:1.2.3.4.3::modifier=delegated.

During authentication, validation checks that the certificate chains to a trusted CA, is within validity, and is not revoked. The authenticator then parses only the defined OIDs/SAN entries, verifies they match allowed schemas and values, and maps them directly to authorization roles and scopes. Any missing, malformed, or unapproved attributes cause authentication or authorization to fail.

- An authorization design that consumes certificate-asserted roles to make access decisions across NGCS/ESInet services, with least-privilege mappings from each role (and modifier) to permissions.

Motorola Response

Comply.

We comply by using an authorization design that consumes roles and modifiers asserted in X.509 certificates and maps them directly to permissions across NGCS/ESInet services. Each role is mapped to a predefined, minimal permission set, and modifiers further constrain those permissions, ensuring access is granted only to the least privilege required for the function.

Our authorization engine (part of the NGCS Policy Store) consumes these certificate-asserted roles to make real-time access decisions.

- Least-Privilege Mapping: Each base role (e.g., Telecommunicator) is mapped to the minimal set of permissions required to answer and route calls.
 - Modifier Adjustments: Modifiers (e.g., Supervisor) dynamically append specific permissions (such as "Listen-In" or "Call Intercept") to the base role without granting broad administrative rights, maintaining a zero-trust posture.
-

- Evidence of baseline role coverage showing agencies exist that assume all baseline agency roles and that no custom roles are required for full system functionality.

Motorola Response

Comply.

We confirm that our deployment supports all NENA-baseline agency roles. Our system is fully functional using only these standardized roles. No custom roles are required for core system functionality, although they may be supported for specialized local PSAP administrative tasks if requested.

- A role registry integration plan (reference NENA-STA-010.3 §10.27 & §10.28) describing how the solution references the Agency and Agent Role registries, maps them to authorization objects, and process registry updates.

Motorola Response

Comply.

Our proposed solution maps authenticated roles to system permissions using strict RBAC and the principle of least privilege. The system's access control policies and virtual hardened oversight ensure that authorized users are mapped and limited only to performing the actions and accessing the system elements required by their specific roles, rights, and permissions. For example, in a multi-tenant environment, the system utilizes role-based partitioning to govern access to logs, call data, and reporting based on the user's assigned role and agency jurisdiction.

- Role lifecycle controls: request to and approval by the superior agency, assignment changes, revocation, and timely de-provisioning; include joiner/mover/leaver workflows for agents' roles.

Motorola Response

Comply.

Our proposed solution provides role lifecycle controls that include formal request submission and approval by the superior agency, controlled role assignment changes, revocation, and timely de-provisioning of access.

The solution incorporates defined joiner, mover, and leaver workflows for agents' roles to ensure access is granted, modified, or removed promptly and in accordance with approved role changes. Joiner, mover, and leaver workflows are established to manage role assignment changes, revocation, and timely de-provisioning. These workflows ensure access is updated or removed promptly when agents join, change roles, or leave.

- Operational procedures for modifiers showing how modifiers adjust privileges without creating new base roles.

Motorola Response

Comply.

Modifiers can add, remove, or change specific privileges on top of an existing base role without creating new base roles. The base role remains unchanged, and access is calculated as base role + active modifiers.

Operational procedure: assign a base role first, then apply one or more modifiers to adjust permissions. Enforce clear rules for modifier scope (what privileges they affect), priority (how conflicts are resolved), and duration (permanent or time-bound). Remove the modifier to immediately revert the user to the original base role permissions.

- Monitoring and audit showing how role use is logged, reviewed, and tied back to the approving superior agency; include alerts for unauthorized role elevation.

Motorola Response

Comply.

Each role event generates a structured log entry capturing user ID, base role, active modifiers, action performed, resource accessed, timestamp, session ID, source system, and outcome (allowed or denied). The log also includes approval metadata such as approving superior agency, approval ID, and validity window, ensuring every action can be traced to an authorized decision.

Logs are written in real time to a centralized, tamper-evident audit store and correlated with authentication and session logs. This allows reviewers to reconstruct who used which role, under what approval, for what action, and whether the role configuration at that moment matched policy.

When unauthorized role elevation is detected, the system immediately logs the event with user ID, the attempted role or modifier, the source, and failure reason. Access is denied, active sessions are terminated if required, and a high-severity alert is sent to security operations and the approving superior agency.

An automated response then enforces containment by removing unauthorized modifiers, locking further elevation attempts, and flagging the account for review. The incident is tracked in the audit system with investigation notes, resolution actions, and final approval or disciplinary outcome.

- Exception handling for temporary/emergency role increases: approval, time bounds, logging, and revocation; include how conflicts between local custom roles and baseline roles are resolved while keeping services available.

Motorola Response

Comply.

In emergency scenarios, the system supports temporary role increases:

- Time-Bound Approval: A supervisor can grant an agent temporary increased roles (e.g., "Mutual Aid Dispatcher") with a mandatory expiration timer.
- Conflict Resolution: If a local custom role conflicts with a baseline NENA role, the baseline NENA role takes precedence for all cross-jurisdictional and ESInet-critical services, ensuring that "security-by-default" is never bypassed during an incident.

4.1.3 Policies and Procedures

The contractor must maintain a comprehensive cybersecurity policy framework for NGCS platforms and the ESInet. Policies may be separate or consolidated, but each required area must have clear purpose, scope, roles, approval, version control, distribution, and compliance expectations. Policies must be approved, communicated to personnel, and reviewed and/or updated on a defined cadence (at least annually or upon material change) to reflect new and emerging technologies, threats, and processes.

Motorola Response

Comply.

Policies must flow down to vendors/contractors/subcontractors and be backed by Standard Operating Procedures (SOPs) that turn policy into repeatable tasks. (e.g., user onboarding, vendor remote access, incident handling, recovery). SOPs must be created, kept current, and used in daily operations.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Policy governance covering ownership, approval authority, versioning, distribution/acknowledgement, training, and review/update cadence.

Motorola Response

Comply.

Ownership and Approval: Security policies are owned and overseen by a dedicated cybersecurity team, comprising over 100 professionals and managed through the NSOC. Any modifications to system policies, network services, or security configurations require formal approval from the Security Manager

Version Control and Distribution: The document control process entails appropriately naming and assigning strict versioning control fields to all project documents, templates, computer files, and other artifacts so that personnel are always using the most current, approved iterations. Information regarding policy updates, scheduled maintenance, or system changes is distributed to authorized stakeholders via the ITSM tool (ServiceNow) and the CWP

Security Awareness Training: All officers, employees, agents, subcontractors, and affiliated users must pass a state-approved criminal background check and complete security awareness training within the past 12 months before gaining access to information technology resources.

Specialized Training: Dedicated NSOC and cybersecurity personnel receive formal security training and hold relevant industry certifications from recognized organizations such as SANS, (ISC)2, and ISACA (e.g., CISSP, CISM)

Review and Update Cadence: To ensure policies and controls reflect new and emerging technologies, threats, and processes, the framework dictates a rigorous review and update cadence. Policies undergo a formal review and update annually or upon major technical or regulatory changes (e.g., NENA i3v4 updates).

- A policy inventory (or consolidated policy) including, at minimum, the policies identified in NENA-STA-040.2 §4.1.2.

Motorola Response

Comply.

Our policy catalog includes all areas mandated by NENA-STA-040.2 §4.1.2.

- Contractual flow-down language proving applicable policies bind all vendors, contractors, and subcontractors supporting NGCS/ESInet.

Motorola Response

Comply.

Our Master Service Agreement (MSA) and standard contracting terms explicitly mandate that all policies, security controls, and operational expectations flow down to any third parties involved in the NGCS/ESInet delivery.

- A complete SOP catalog mapped to the above policies.

Motorola Response

Comply.

We maintain a detailed SOP Catalog where every technical task is mapped back to its parent policy. For example:

- **Policy: Access Control** → SOP: User Provisioning/Deprovisioning (Joiner/Leaver).
 - **Policy: Vulnerability Management** → SOP: Monthly Security Patching via AdminiStation.
 - **Policy: Incident Response** → SOP: Notification Escalation to the State.
-

- SOP governance describing authorship, approval, version control, authoritative storage, and periodic update cycle; include triggers for out-of-band updates (e.g., new technology implementation or threat vectors).

Motorola Response

Comply.

Our SOP guidance outlines the following principles and governance arrangements that are in place when developing SOPs.

- **Authorship & Strict Approval:** Proposed modifications to system policies, configurations, or SOPs are rigorously assessed by our engineering staff for risk, impact, and cost. No operational changes are executed without formal authorization from an CSM, a Change Advisory Board (CAB), and designated client stakeholders.
 - **Centralized Version Control:** All critical SOPs, configuration files, and templates are maintained within a centralized, authoritative repository. Strict naming and version control protocols guarantee that our personnel and clients are always referencing the most current, approved procedures.
 - **Scheduled Review Cadence:** We maintain our system baseline through rigorous, scheduled audits. Operational plans are reviewed on a mutually agreed cadence, baseline security controls and ACLs undergo mandatory quarterly true-ups, and comprehensive NIST-based risk assessments are conducted annually.
 - **Expedited Out-of-Band Updates:** To proactively address urgent requirements outside of scheduled maintenance windows, we utilize an Emergency Change Request process. This rapid-deployment protocol is triggered by critical events such as zero-day security patches, post-incident root-cause mitigations, or the required implementation of newly ratified industry standards (e.g., incorporating NENA i3 updates within 18 months).
-

- Training and attestation evidence showing personnel have been informed of relevant policies and procedures.

Motorola Response

Comply.

We ensure that all personnel are informed of relevant policies and procedures through a structured training program, with evidence of completion and attestation tracked formally. Personnel assigned to the Nebraska project must complete mandatory Security Awareness Training upon onboarding and annually thereafter. Evidence is provided via transcripts from our Learning Management System (LMS), showing 100% completion rates and signed attestations for all relevant policies and SOPs.

- Compliance and exception processes describing how adherence is monitored; how exceptions/waivers are requested, risk-assessed, time-bounded, approved; and how they are revisited/closed.

Motorola Response

Comply.

Motorola ensures strict adherence to cybersecurity and operational policies, actively managing exceptions through continuous monitoring, standardized risk assessments, and an ITIL-based Change Management framework.

Compliance and exception management process include:

- **Continuous Monitoring & Auditing:** System adherence is monitored 24x7x365 by our NSOC using advanced SIEM tools. Compliance is further assured through quarterly baseline validations and independent third-party audits (ISO 27001 and SOC 2 Type 2).
 - **Standardized Risk Assessment:** Any discovered exceptions to baseline controls are immediately evaluated using the NIST SP 800-30 framework and documented within our Quarterly Risk Assessment Reporting (QRAR).
 - **Time-Bounded Remediation:** Exceptions are not left open indefinitely; they are actively managed via formal service change requests. Critical vulnerabilities trigger an Emergency service change request service change request to immediately expedite the remediation timeline.
 - **Strict Approval Governance:** All mitigations and RFCs require formal review and approval by a Change Advisory Board (CAB) and designated client stakeholders. This process establishes an exact, approved schedule, effectively time-bounding the exception.
 - **Validation & Closure:** Following the deployment of a fix, the system undergoes a rescan and revalidation of controls. A Post Implementation Review (PIR) is then conducted to verify success and formally close the change request and its associated exception.
-

- Cross-references showing how policies and SOPs align with the Risk Management program and Incident Response, ensuring non-compliance items route to corrective action and/or formal risk acceptance.

Motorola Response

Comply.

Motorola ensures the seamless alignment of our policies and SOPs with our Risk Management and Incident Response programs through a highly integrated, ITIL-based framework. Our Cybersecurity Risk Management Framework is built upon industry-leading best practices and leverages standards such as ISO 27001, ISO 31000, NIST SP 800-30, NIST SP 800-53, and the NIST Cybersecurity Framework.

To maintain the highest levels of security and compliance, our system utilizes continuous monitoring, quarterly audits, and a strictly structured change management process. This rigorous approach guarantees that any non-compliance items, vulnerabilities, or security exceptions are systematically identified and routed directly to corrective action or formal risk acceptance.

Key elements of our integrated approach include:

- **Incident Response Alignment:** Continuous improvement is built into our incident response cycle. If an SOP fails or underperforms during a security or operational incident, the resulting After-Action Report (AAR) automatically triggers a mandatory review and update of the associated policy to prevent recurrence.

- **Accountable Corrective Action:** Vulnerabilities or process gaps identified during internal audits or penetration tests are immediately routed to a Plan of Action and Milestones (POA&M). This strict tracking system ensures that non-compliance items are never "lost" or overlooked, but are instead actively managed as formal risks and tracked through to successful closure.
-

4.1.3.1 Incident Response Plans

Early detection and disciplined response are essential to protect NG911 operations. Detection should use tooling (e.g., SIEM, IDS/IPS) and informed personnel, with trained staff triaging scope and impact. The contractor must maintain a formal, written **Cybersecurity Incident Response Plan (CIRP)** that is adaptable, periodically evaluated and tested, and staffed by trained responders. The CIRP should follow **Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity** and define when and how to engage external resources.

Motorola Response

Comply.

Because NG911 must continue answering calls and dispatching responders even under attack, recovery planning must be rigorous. The contractor must maintain **Business Continuity (BC)** and **Disaster Recovery (DR)** plans (separate or combined; separate recommended), store all plans offline yet accessible to recovery teams, and review/test at least annually, updating plans as needed.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A CIRP aligned to Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident Activity, with incident declaration/classification criteria and communications/notification procedures.

Motorola Response

Comply.

Motorola maintains a formal CIRP aligned with NIST 800-61 r2 and NENA NG-SEC standards. The plan follows the standard lifecycle:

- Preparation (baseline security and training)
- Detection & Analysis (triage of SIEM/MDR alerts)
- Containment, Eradication & Recovery (limiting spread and restoring clean state)

- Post-Incident Activity (after-action reviews)

We utilize specific Incident Declaration criteria (e.g., loss of PII, disruption of call routing) and defined Communication/Notification procedures to ensure the Motorola NSOC is alerted within established SLAs.

- Detection capabilities and processes showing how SIEM, IDS/IPS, and staff reports enable early detection; include triage workflows, severity classification, and criteria to escalate to incident status.

Motorola Response

Comply.

Motorola's 24x7x365 NSOC serves as the central hub for monitoring, detecting, and managing incidents across the Next Generation 9-1-1 (NG9-1-1) system. The system utilizes a combination of automated security tools and staff-initiated reporting to enable early detection, structured triage, and standardized incident escalation.

Detection Capabilities (SIEM, IDS/IPS, and Staff Reports)

- **SIEM** : The NSOC continuously monitors network traffic, system logs, and security alerts in real-time. Advanced SIEM tools are used to correlate these security events, track operational system metrics, and identify potential cyber threats or network anomalies early.
- **IDS/IPS (Intrusion Detection/Prevention Systems)**: Deployed throughout the ESInet, IDS/IPS solutions provide signature-based monitoring and deep-level packet inspection to detect and mitigate malicious activity. This is supplemented by machine learning algorithms that identify unusual network traffic patterns or behaviors indicative of a potential attack.
- **Staff and User Reports**: In addition to automated alarms, the incident management system captures support requests reported by users. Authorized PSAP staff can report incidents directly to the NSOC via a dedicated toll-free number, email, or the CWP. Telephone reporting is strictly required for Critical and High-priority incidents to ensure immediate action.

Triage Workflows When an alert is generated or a user reports an issue, the NSOC follows a defined triage and problem-resolution workflow:

- The NSOC receives the request, documents the circumstances, and opens a case in the ITSM tool, ServiceNow.
 - Engineers assess the criticality of the issue and assign a Severity Level classification, which prioritizes the request.
 - The NSOC performs remote analysis and diagnostics to identify a corrective action plan and begin troubleshooting immediately.
 - If the incident cannot be resolved remotely, the NSOC dispatches on-site support engineers
-

- Training and exercise evidence for personnel with plan duties and proof the CIRP is tested (tabletop/live); include after-action reviews and documented improvements.

Motorola Response

Comply.

We provide evidence of readiness through a rigorous Cyber Exercise Program. This includes annual tabletop exercises and live "red-team" simulations designed to test the CIRP under pressure.

We ensure peak system resilience and response capabilities through a continuous cycle of rigorous training, proactive testing, and structured incident reviews.

- **Expert Personnel:** Our 24x7x365 NSOC staff undergo rigorous initial and ongoing training to resolve critical 9-1-1 issues. Dedicated security personnel hold top-tier industry certifications (e.g., SANS, (ISC)², ISACA), and all employees complete regular security awareness training.
 - **Proactive Plan Validation:** We do not wait for emergencies to test our readiness. Our DR/BC, and Continuation of Operations (COOP) plans require strict, regularly scheduled validation exercises to ensure restoration processes are highly effective.
 - **Continuous Improvement (AARs):** Following any incident or outage, we conduct a formal After-Action Review (AAR) and root cause analysis. Findings are transparently documented in an Event Analysis Report (EAR) provided to the customer, detailing the timeline, conclusions, and specific preventative measures implemented to ensure the issue does not recur.
-

- A Business Continuity (BC) Plan for maintaining critical services during and after disruption.

Motorola Response

Comply.

We comply with this requirement by maintaining a comprehensive BC specifically designed for maintaining critical services during and after a disruption.

Our mission and the primary goal of our BC is to provide ongoing, continuous customer support and operational services despite any significant business disruptions, including the loss or degradation of normally available business systems, facilities, or other vital resources.

To guarantee the effectiveness of our continuity planning, we strictly adhere to globally recognized standards. Motorola follows the practices documented in ISO 22301 as our primary guideline, and successfully achieved official International Standards Organization (ISO) Certification for "Security and resilience — BC management systems — Requirements" on June 12, 2022.

- A Disaster Recovery (DR) Plan detailing IT restoration and coordination with ongoing mission-critical operations.

Motorola Response

Comply.

We maintain a comprehensive DR Plan designed to ensure continuous mission-critical operations and rapid IT restoration during unforeseen disruptions. They are critical to the security of our NGCS networks and are only released under very specific non-disclosure conditions, which we will discuss

with the State upon request. Below, we have summarized the pertinent non-proprietary key points for the State to understand the scope and general depth of the plans.

IT Restoration and Backup Procedures: The DR plan formally defines specific RPOs) and RTOs for critical data and system functionality, alongside step-by-step procedures for recovering systems and data.

- **Active/Active Environments:** Services are deployed using a multi-cloud structure with an Active/Active architecture to ensure high availability.
 - **Backup Scheme:** Full backups of all systems are performed using a rigorous "grandfather-father-son" backup schedule. Additional backups are taken whenever configuration changes are made.
 - **Tactical Snapshots:** Point-in-time snapshots are utilized before and after any system change events to provide a working copy for immediate rollback/restoration if a failure occurs during maintenance.
-

- Plan maintenance & accessibility controls proving CIRP/BC/DR are maintained offline yet readily accessible to recovery teams, with clear ownership, version control, and distribution.

Motorola Response

Comply.

We ensure that all Cyber Incident Response Plans (CIRP), BC, and DR plans are securely managed, strictly version-controlled, and highly accessible during a crisis.

- **Secure Storage & High Availability:** Plans are maintained in a secure, centralized digital vault. To guarantee availability during severe network-wide outages, recovery teams are equipped with offline-accessible copies via encrypted portable storage.
 - **Clear Ownership & Execution:** Ongoing planning and execution are owned by site-specific Business Continuity Teams (BCT) and the Security Manager. During a significant disruption, an Emergency Management Organization (EMO) assumes command to direct specialized response teams and restore vital infrastructure.
 - **Strict Version Control:** All operational plans and templates utilize strict naming conventions and formal "versioning control fields." This centralized repository ensures that recovery teams are always operating from the most accurate, authoritative procedures.
 - **Resilient Communications:** The distribution of critical information is governed by a detailed Escalation and Notification plan. This establishes primary and secondary communication methods (in-person, phone, text, and email) to ensure seamless coordination regardless of the disruption.
 - **Client Review:** To protect our overarching network security, the full COOP and DR plans are highly proprietary. However, they are readily available to the State for detailed review under a Non-Disclosure Agreement (NDA).
-

- Review and test cadence showing at least annual reviews/tests of CIRP/BC/DR, with triggers for interim updates and documented results.

Motorola Response

Comply.

We mandate rigorous annual testing and regular reviews of all Cyber Incident Response (CIRP), BC, and DR plans. To ensure our response strategies remain current, we also trigger interim plan updates in response to significant system changes, newly identified threat vectors, or findings from an After-Action Review (AAR).

Review and Testing Cadence

- **Annual Assessments & Audits:** We conduct comprehensive vulnerability scans and NIST SP 800-30 based security risk assessments annually.
- **BC/DR Validation:** We utilize a continuous "Plan-Do-Check-Act" methodology to ensure that disaster readiness and communication protocols are regularly tested, evaluated, and improved.
- **Quarterly Security Reviews:** To maintain strict security hygiene, all physical and logical s ACLs and baseline security controls undergo mandatory quarterly true-ups.

Documented Results and Transparency

- **Post-Incident Reporting:** Following an incident or outage, we provide the customer with complete transparency. A preliminary Reason for Outage (RFO) is delivered rapidly, followed by an in-depth Event Analysis Report (EAR) detailing the full timeline, root-cause analysis, and specific corrective actions.
 - **Audit Documentation:** The results of our security testing and operational compliance are formally documented. These documents validate our system's security, privacy, and processing integrity and are available to the procuring agency upon request.
-

- Containment and recovery playbooks/SOPs translating plans into actionable steps for common scenarios (malware/ransomware, denial of service, critical service outage), including initial containment, eradication, service restoration, and lessons learned.

Motorola Response

Comply.

Our NSOC employs a mature, structured Incident Management Policy to rapidly address security threats and service disruptions. Our methodology follows four strict operational phases: Containment, Eradication, Service Restoration, and Lessons Learned.

To ensure swift and precise action, the NSOC utilizes predefined playbooks for critical scenarios:

Malware/ransomware and Denial of Service:

- **Malware & Ransomware:** Utilizing predictive Host-based Intrusion Detection Systems (HIDS), the NSOC detects threats in real time, instantly isolates affected network zones to prevent lateral movement, and eradicates malicious code. Services are rapidly restored to a clean state using rigorous point-in-time Virtual Machine (VM) snapshots.

- **DDoS & TDoS Attacks:** We defend against volumetric DDoS via active traffic scrubbing, firewalls, and rate-limiting. For Telephony DoS (TDoS) targeting 9-1-1 queues, our SBCs reject malformed SIP calls, while core systems isolate suspected malicious traffic into dedicated queues—ensuring legitimate 9-1-1 calls are always prioritized and answered.

Critical Service Outages:

- **Network/Component Failure:** Our NGCS rely on a redundant, multi-cloud microservices architecture. If a failure occurs, the Software Defined Network (SDN) automatically steers traffic to healthy regions without human intervention.
- **Facility Evacuation:** The PSAP Abandonment option in the CWP instantly triggers PRRs to reroute calls to alternate PSAPs. In the event of total local infrastructure destruction, agencies can deploy our secure, optional browser-based VESTA NXT Continuity call handling solution over any standard internet connection.

Post-Incident Transparency & Continuous Improvement:

Following service restoration, our incident management system triggers a formal reporting cycle to identify root causes and implement preventative measures. We provide complete transparency through:

- **Reason for Outage (RFO):** A preliminary incident report delivered to the customer
- **Event Analysis Report (EAR):** A comprehensive root-cause analysis is provided detailing the full event timeline, conclusions, and specific recommended actions to prevent future occurrences.

-
- External assistance procedures specifying when/how outside help is engaged, required approvals, and current contact lists/resources.

Motorola Response

Comply.

We manage the engagement of external assistance, including third-party suppliers, network partners, and field technicians, through a centralized project and service management framework. Motorola serves as the single point of contact and assumes accountability for all external resources used within the NG9-1-1 service.

Here is how external assistance is governed, approved, and accessed:

When and How Outside Help is Engaged

- **Third-Party Suppliers and Network Partners:** We utilize specialized external partners for specific system components, such as telecommunications aggregators, IP network providers, and local "smart hands" deployment vendors.
- **Centralized Coordination:** To minimize the administrative burden on the customer, Motorola's Project Manager (PM) or designated CSM handles all direct communication, scheduling, and oversight of these external suppliers.
- **Expedited Issue Resolution:** If a technical issue requires specialized knowledge from a third-party supplier, the Motorola PM proactively facilitates direct access between the customer and the appropriate technical resources via calls, virtual meetings, or on-site support.

- **Field Dispatch:** During live operations, if the NSOC cannot resolve an issue remotely, the NSOC or the Operations Support Manager will automatically dispatch local technical support or local "smart hands" for on-site hardware replacement or repair.

Required Approvals

- **Subcontractor Substitutions:** We maintain strict control over our external resources. Contractually, we cannot substitute or replace our designated supplier without the prior written consent of the customer.
- **Removal of Suppliers:** If the customer determines at any time that an external resource is unacceptable, they should notify Motorola. Motorola will take the appropriate steps to provide a qualified replacement.
- **Change Management:** If an external partner needs to make a service-impacting change or routine maintenance update to the network, it must go through our ITIL-based Change Management Process. A service change request is submitted and must receive formal approval from the Change Advisory Board and designated customer stakeholders before the external party is authorized to execute the work.

Current Contact Lists and Resources are maintained to ensure timely responses during incidents and escalations involving external or internal resources, we provide a standardized escalation contact matrix within our Customer Support Plan (CSP).

The current contact progression for incidents is:

- Initial Contact (Tier 1):
 - NSOC
 - Phone: 1-800-881-4245 (Available 24x7x365. Option 4, 1, 2 for emergencies).
 - Email: VestaNSOC@motorolasolutions.com (For low-priority/administrative inquiries only).
 - 1st Escalation (Tier 2 - NSOC Management):
 - Michaela Johnson, Senior Manager, Network & Security Operations
 - Phone: 303-246-7119
 - Email: Michaela.Johnson@motorolasolutions.com.
 - 2nd Escalation (Tier 3 - Technical Support & Service Delivery):
 - Heidi Pickett, Senior Manager, Technical Support Operations
 - Phone: 925-596-3379
 - Email: Heidi.Pickett1@motorolasolutions.com.
 - Additional NGCS Operations Escalations:
 - Steve Gissen, NGCS Operations Manager
 - Phone: 303-775-0289
 - Email: Steve.Gissen@motorolasolutions.com.
 - Jim Stowe, Director of NGCS Operations
 - Phone: 858-518-6049
 - Email: Jim.Stowe@motorolasolutions.com.
-

4.1.4 Authorization and Data Rights Management

The contractor must enforce **XACML 2.0-based authorization** for all NG911 interfaces and protected data. Policies must evaluate **subject, resource, action, and context attributes**; be stored in a **Policy Store** (§E-2.2.1.1); decided by a **Policy Decision Point (PDP)**; and enforced at a **Policy Enforcement Point (PEP)**. Interfaces and data must use consistent names (NENA-STA-010.3 §10, et seq.). Actions must be explicit – **Read, Create, Update, Delete, Execute** – with **permit/deny rules** and an **explicit default rule** for every policy set.

Motorola Response

Comply with Clarification.

While NENA i3 historically referenced XACML for policy expression, Motorola has adopted OAuth 2.0 and OpenID Connect (OIDC) as the primary framework for identity and access management. This alignment reflects the broader industry shift toward more performant, JSON-native security architectures that provide superior interoperability within the ESInet.

Provisioning data is owned by the agency that operates the element and must be governed by data rights management. Each XACML policy must be packaged as a JWS and signed by the policy owner, including the signing certificate and full chain for validation.

Motorola Response

Comply with Clarification.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Authorization architecture showing XACML 2.0 components, PDP placement, and how authorization is invoked on all NGCS/ESInet interfaces and protected data paths.

Motorola Response

Comply with Clarification.

- Policy naming conventions & registries usage, including:
 - Interface policy names derived from `ServiceID`, and an interface keyword (NENA-STA-010.3
 - §10.30) formatted `ServiceID~keyword`(e.g., `LoST~ecrf.state.pa.us`)
 - Data item names derived from OpenAPI JSON object names and optional element tags, using dot notation (e.g., `civicAddr.A3`, or `<eido.AgencyDataComponent.AgencyName>`)
 - Mapping to the Policy Type Registry (NENA-STA-010.3 §10.33)

Motorola Response

Comply with Clarification.

- Action model defining Read, Create, Update, Delete, Execute, with examples showing how each applies to representative Interfaces and data structures.

Motorola Response

Comply with Clarification.

- Example XACML policy sets for:
 - One or more interfaces
 - One or more data structures
 - Each example policy set provided must include permit/deny rules, an explicit default rule, and attribute conditions (subject/resource/action/date/time as applicable).

Motorola Response

Comply with Clarification.

- JWS packaging & validation: how the policy owner signs policies; how the certificate and chain are included (by value or reference); how PEP/PDP validate signatures (CRL/OCSP) and how key rotation and revocation are handled.

Motorola Response

Comply with Clarification.

- Data rights management procedures establishing ownership of provisioning data and how ownership is enforced in policy.

Motorola Response

Comply.

We support clear data ownership boundaries to ensure the absolute protection and sovereignty of your agency's information.

- **Exclusive Customer Ownership:** You retain full title, ownership, and exclusive rights to all data or records generated as a direct result of the service contract.
- **Motorola Intellectual Property:** Motorola retains exclusive ownership of our pre-existing intellectual property, software code, algorithms, and background materials used to deliver NG9-1-1 services.

- **Strict Purpose Limitation:** We access and utilize your data solely to fulfill contractual obligations, resolve technical issues, or respond to your direct written requests. Unauthorized copying, disclosure, retention, or secondary use of customer data is strictly prohibited.
 - **Least Privilege Access:** Only duly authorized personnel are permitted to access customer data, and we strictly this access to the degree necessary to accomplish the requested services.
 - **End-of-Contract Disposition:** Upon contract termination, you dictate how your data is handled. You may extract the data using provided tools, require a formal return of all data, or mandate secure, permanent destruction in strict accordance with NIST SP 800-88 "Media Sanitization Guidelines" (accompanied by a formal Certificate of Destruction).
-

- Policy lifecycle controls: authoring, peer review, change management, pre-production testing/evaluation, promotion, versioning, rollback, archival; include who is authorized to sign and publish policies.

Motorola Response

Comply.

We govern all system modifications and policy updates using a rigorous, ITIL-based Change Management framework. This zero-disruption approach ensures every change is systematically tested, documented, and controlled to protect mission-critical 9-1-1 operations.

- **Initiation & Authoring:** Authorized agency personnel or Motorola staff initiate service change request. For routing policies, authorized PSAP administrators can seamlessly view or request modifications directly via the CWP.
 - **Peer Review & CAB Assessment:** Every service change request undergoes a comprehensive peer review to evaluate impact and risk. Our Cybersecurity team actively participates in the Change Advisory Board (CAB) to assess all security implications prior to approval.
 - **Pre-Production Testing:** Before promotion, an implementation plan and Method of Procedure (MOP) are developed. The proposed change is rigorously validated using simulated traffic within a production-parity lab environment.
 - **Mandatory Rollback & Execution:** A back-out plan is mandatory. Prior to execution, tactical Virtual Machine (VM) snapshots are captured to preserve the pre-change state, guaranteeing immediate system restoration if unforeseen issues arise during promotion. All configurations are stored in a centralized, strictly version-controlled repository.
 - **Collaborative Authorization:** Authority to publish is strictly collaborative. Final scheduling requires explicit sign-off from designated client stakeholders, the Motorola Change Manager (via ServiceNow), and the CAB. Crucially, no non-emergency changes are ever performed without prior notice and mutual agreement.
 - **Archival & Post-Implementation Review (PIR):** Following implementation or rollback, the results are documented in a formal PIR and permanently archived to support forensic audits, problem management, and continuous lifecycle improvement.
-

- Logging & auditability: decision logs at PEP/PDP, retention, and procedures for reviewing denied/exception events.

Motorola Response

Comply.

PEP/PDP Logging: The Policy Decision Point (PDP) evaluates policies, and the Policy Enforcement Point (PEP) enforces access decisions across all NG9-1-1 interfaces. All access decisions (Permit/Deny) and actions (Read, Create, Update, Delete, Execute) are logged directly at the PEP/PDP to maintain a comprehensive audit trail.

Retention: All event logs, including PEP/PDP decision logs, are securely stored and retained based on retention policies.

Reviewing Denied/Exception Events: The system captures denied access attempts and exception events at the PEP/PDP. Authorized personnel can review these events through role-based reporting tools, and a Discrepancy Reporting (DR) mechanism formally tracks, investigates, and resolves security, permissions, and authentication exceptions.

- Performance & availability targets: PDP availability/latency, decision/policy caching (TTL/invalidations), and fail-secure behavior if policies or validators are unavailable.

Motorola Response

Comply.

Performance & Availability Targets: The Policy Decision Point (PDP) and NGCS elements are deployed in a highly available architecture targeting 99.999% availability.

Decision/Policy Caching (TTL/Invalidations): Policies retrieved from the Policy Store are valid only until their designated expiration time. Once expired, the policy must be retrieved again from the Policy Store to be used.

Fail-Secure Behavior: Every policy rule set requires an explicit default rule. If a policy cannot be retrieved, the rule securely fails by evaluating to 'false', and the system progresses to the next lower-priority rule or a provisioned default queue to ensure continuous call processing.

4.2 Information System Infrastructure and Management

4.2.1 Device Inventory

The contractor must maintain a **continuously updated inventory** of all **devices, software/applications, software libraries, data sets, and cloud/third-party services** that support the NGCS platform and the ESInet. Use automated discovery and reconciliation where possible to keep records accurate, quickly identify unauthorized items, verify patch/firmware levels, and support zoning/segmentation. If full visibility is limited by span of control or contracts, clearly define what is in scope, assumptions, and responsibilities. Inventory outputs must inform critical impact analysis (BC/DR inputs) and drive trusted vs. untrusted zone design and controls at all ingress/egress points.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Inventory management approach describing data sources, automated discovery tools/processes (where used), manual reconciliation, update frequency, and how unauthorized/unknown items are identified and removed or quarantined.

Motorola Response

Comply.

Data Sources & Discovery: We utilize a hybrid approach combining automated discovery and systematic logging. Our NSOC employs tools such as SNMP-based scanners and agent-based endpoint detection to automatically identify and catalog network elements (routers, firewalls, servers).

Reconciliation: Automated scans are subjected to manual reconciliation monthly to ensure virtualized instances and offline spares are correctly attributed.

Unauthorized Item Handling: Unknown items are identified via MAC-address filtering and 802.1X authentication. Any unauthorized device is automatically quarantined into a non-routable VLAN, triggering an immediate "Critical" alert in the NSOC for investigation.

- Scope and span-of-control statement clarifying which assets/services fall under the Provider vs. the Customer or other vendors; include contractual boundaries, dependencies, and any blind spots.

Motorola Response

Comply.

Provider (Motorola) Responsibility: All core NGCS FEs (ECRF, LVF, ESRP), BCF, and the primary ESInet backbone.

Customer (State/PSAP) Responsibility: PSAP-side CPE, local area networks (LANs), and agency-owned workstations.

Contractual Boundaries: The demarcation point is typically the hand-off port at the PSAP call handling host edge router. Dependencies include OSP connectivity, which is monitored but not directly controlled by Motorola.

- Comprehensive inventory documentation should identify sufficient detail – at minimum, documenting inventory elements identified in NENA-STA-040.2 §5.4 – for all aspects of NGCS and ESInet infrastructure. Classification linkage showing how inventories map to the provider's data classification policy and define required protections.

Motorola Response

Comply.

Our inventory documentation captures all elements identified in NENA-STA-040.2 §5.4, including:

Identity: Make, model, serial number, and UUID.

Configuration: OS version, firmware level, and last patch date.

Networking: Static/Dynamic IP addresses, MAC addresses, and physical/logical port mapping.

Physical Location: Data center rack/RU position or PSAP site ID.

- Classification linkage showing how inventories map to the provider's data classification policy and define required protections.

Motorola Response

Comply.

Every item in the inventory is mapped to the Data Classification Policy.

Required Protections:

- Asset's processing PII or call-signaling (e.g., EIDOs) are classified as "**High Sensitivity**" and require mandatory encryption at rest, mTLS authentication, and 24/7 logging.
 - Assets serving **public-facing** functions (e.g., external ECRF) receive specialized DDoS and WAF protections.
-

- Impact analysis methodology showing how the inventory feeds critical impact analysis and integrates with Business Continuity and Disaster Recovery planning.

Motorola Response

Comply.

BCDR Integration: The inventory serves as the foundational data source for the Business Impact Analysis (BIA).

By mapping application dependencies (e.g., "ECRF relies on Database Cluster A"), we can predict the impact of a specific hardware failure. This data feeds directly into our DR orchestration, ensuring that high-impact assets are prioritized for restoration in geo-redundant failover scenarios.

- Zoning/segmentation mapping that uses the inventory to define trusted vs. untrusted zones and sets control placement and rule scope at all ingress/egress points.

Motorola Response

Comply.

We use the inventory to enforce micro-segmentation.

Trusted vs. Untrusted: The ESInet is partitioned into zones (e.g., Management Zone, Core Service Zone, Agency Zone).

Control Placement: BCFs and internal firewalls use the inventory as the "authoritative list" for rule scope. Any IP/device not present in the inventory is denied communication between zones, setting a hard boundary at all ingress/egress points.

- Governance & lifecycle controls for the inventory: ownership, update cadence, audit/attestation of accuracy, change triggers, reconciliation with change management processes, and evidence of periodic cleanup of stale records.

Motorola Response

Comply.

Ownership: The Security Administrator is the primary owner of the inventory database.

Update & Audit: The inventory is updated in real-time upon any change management event. We conduct an annual attestation of accuracy where site technicians physically verify 10% of random assets.

Cleanup: Stale records (decommissioned assets) are archived after 90 days of inactivity to ensure the production inventory remains clean and actionable.

4.2.2 Patching and Update Management

The contractor must implement a disciplined, **change-managed patching program** covering **firmware, hardware drivers, operating systems, applications, and middleware**. The program must take in vendor, CERT, or other security advisories, use a common severity scale (e.g., Common Vulnerability Scoring System [CVSS]) to set priority, and check the environment for indicators of compromise (IoC) when a vulnerability is disclosed. Patching must be timely and paired with post-patch verification. The program should align with timelines and processes defined in NENA-STA-040.2 §5.5.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A process to validate – at least monthly – that all required patches are installed across in-scope hardware and software (plus event-driven checks upon major vulnerability disclosures).

Motorola Response

Comply.

Motorola performs monthly validations to ensure that all in-scope hardware and software components are up to date with the latest security definitions and patches. In addition to this scheduled cadence, our NSOC triggers event-driven checks immediately upon the disclosure of major vulnerabilities (e.g., zero-day exploits) that could impact the ESInet or NGCS core.

- A change-managed deployment workflow ensuring approved and appropriately tested mitigations/patches are applied as soon as possible, with defined rollback steps.

Motorola Response

Comply.

We follow a rigorous Change Management workflow for all updates:

- **Testing:** All patches are first applied in our dedicated Information Assurance lab, which mirrors the production NG9-1-1 environment. This identifies potential interactions or reboot requirements before they affect live services.
 - **Deployment:** Approved patches are deployed during maintenance windows using standardized tools (e.g., AdminiStation).
 - **Rollback:** Every change includes a documented rollback plan. If post-patch performance issues arise, technicians can quickly revert the system to its pre-patch state using the last-known-good configuration and snapshot backups.
-

- Post-patch verification to confirm remediation and to check for exploitation and/or other IoCs across the ESInet and NGCS.

Motorola Response

Comply.

Following any patch application, we conduct post-patch verification to confirm successful remediation. This process includes:

- **Remediation Confirmation:** Automated scanning to verify the vulnerability is no longer exploitable.
 - **IoC Scanning:** Our service and process checks for Indicators of Compromise (IoCs) and signs of exploitation across the ESInet and NGCS core. This ensures that no malicious activity occurred during the window between vulnerability discovery and patch deployment
-

- A CVSS-based timeline policy that sets SLAs by severity/criticality (e.g., critical expedited; target ≤ 48 hours from disclosure or patch availability), and an emergency change path.

Motorola Response

Comply.

Our patching policy sets strict SLAs based on CVSS (Common Vulnerability Scoring System) scores:

- **Critical (9.0–10.0):** Expedited remediation, with a target of ≤ 48 hours from patch availability or the implementation of an emergency change path for high-risk exploits.
 - **High (7.0–8.9):** Remediation typically occurs within 7–14 days.
 - **Medium/Low:** Patches are bundled into the next monthly maintenance cycle.
-

- Evidence of advisory intake and triage, including how severity, affected scope, available mitigations, and permanent vs. temporary fixes are evaluated and tracked.

Motorola Response

Comply.

The NSOC maintains a continuous advisory intake process, monitoring sources such as CISA, MS-ISAC, and vendor-specific portals.

- **Triage:** Each advisory is evaluated for severity, affected scope within the State of Nebraska ESInet, and available mitigations.
 - **Tracking:** We track both permanent fixes (patches) and temporary mitigations (e.g., firewall rule adjustments) until the permanent solution can be safely applied and verified.
-

- Exception handling with compensating controls when patches cannot be applied immediately, with documented risk acceptance under the Entity's risk management process.

Motorola Response

Comply.

When a patch cannot be applied immediately due to operational risks (e.g., a "vital to communication" concern), we initiate an Exception Handling process.

- **Compensating Controls:** We implement temporary security measures, such as enhanced IDS/IPS signatures or restricted network access, to mitigate the risk.
 - **Risk Acceptance:** These exceptions are documented, risk-assessed, and submitted for formal risk acceptance by the State's risk management authority, with a mandatory re-evaluation date.
-

- Reporting and metrics showing patch compliance, age of open findings by CVSS band, time-to-patch, and reconciliation with the inventory/CMDB to ensure complete coverage.

Motorola Response

Comply.

Motorola provides a monthly service report which includes information related to patch deployment. These metrics include:

- **Compliance Percentage:** Proportion of assets fully patched against the baseline.
 - **Age of Findings:** Number of days open vulnerabilities have existed, grouped by CVSS band.
 - **Time-to-Patch:** Average time from disclosure to remediation.
 - **Reconciliation:** All reports are cross-referenced with the Device Inventory/CMDB to ensure 100% coverage across all physical and virtual NG9-1-1 assets.
-

4.2.3 Segmentation and Traffic Separation

The contractor must implement **domain-level network segmentation** to contain incidents, reduce lateral movement, and improve resiliency. Segmentation may be physical or logical (e.g., firewall-enforced choke points) and should extend to **zero-trust/micro-segmentation** at the endpoint or workload wherever feasible. Production and non-production (test/training) must be strictly separated so non-production activity cannot affect production services. **Development tools are prohibited in the production environment.** Within each environment, distinct traffic classes (e.g., call/signaling, management/monitoring, administrative) must be segregated and filtered (VLANs and/or dedicated equipment) with explicit allow-lists and firewall policy. Management/monitoring traffic must be out-of-band, normal traffic must not use the default VLAN, and configuration access to traffic-handling devices must use administrator-level accounts under appropriate controls.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A segmentation architecture showing production vs. non-production separation, inter-segment demarcation points, and isolation/containment controls.

Motorola Response

Comply.

Motorola utilizes a "Zero Trust" zoning model to separate production from non-production (Development/Staging) environments.

- **Production Segment:** Houses live NGCS FEs (ECRF, LVF, ESRP) which are logically isolated via hardened BCF.
 - **Non-Production Segment:** A physically distinct environment for testing and staging.
 - **Demarcation & Isolation:** Inter-segment traffic is strictly prohibited. Isolation is enforced through stateful firewalls and data controls at the management boundary, ensuring that testing activities never traverse production pathways.
-

- A traffic separation design identifying major traffic classes and how they are segregated and filtered.

Motorola Response

Comply.

We categorize traffic into major classes to apply granular filtering:

- **9-1-1 Emergency Traffic:** Prioritized SIP/RTP/MSRP traffic from OSPs.
 - **Management Traffic:** Secure SSH/HTTPS traffic for system administration.
 - **Monitoring/Logging:** UDP/TCP streams for SIEM and health telemetry.
 - **Segregation:** Traffic is segregated using VLAN tagging (802.1Q) and dedicated VRFs (Virtual Routing and Forwarding) at the core routers. Filtering is performed at every ingress/egress point via ACLs that only permit recognized "Traffic Class" signatures.
-

- Evidence that production is protected from non-production, including controls preventing any non-production impact on production systems, and an explicit statement that no development tools exist in the production environment.

Motorola Response

Comply.

Motorola confirms that no development tools exist within the production environment. Production systems are built from verified images that have undergone regression testing in non-production. Controls include mandatory code signing and the absence of compilers, debuggers, or IDEs in live segments to minimize the attack surface.

- Out-of-band management/monitoring implementation details and confirmation that normal traffic is not on the default VLAN.

Motorola Response

Comply.

Administrative and monitoring traffic is carried over a dedicated Out-of-Band (OOB) management network.

VLAN Configuration: We confirm that normal traffic is never carried on the default VLAN. Management interfaces utilize a non-standard, secure VLAN (VLAN 999 or similar) with independent physical ports (LOM/iDRAC) where possible, ensuring that a congestion event or attack on the production network does not block administrative access.

- Administrative access controls for traffic-handling devices: administrator-level account use, authorization model, MFA, logging, and audit.

Motorola Response

Comply.

Access to traffic-handling devices (routers, BCFs) is strictly controlled:

- **Identity:** All administrators use individual, non-generic accounts linked to the Agency Identity Provider.
 - **Authorization:** RBAC ensures administrators only have the permissions necessary for their specific duty (Least Privilege).
 - **MFA:** MFA is mandatory for all administrative logins.
 - **Audit:** Every keystroke and configuration change are logged in a tamper-proof audit trail within the central SIEM.
-

- Operational procedures/SOPs for change, testing, and validation of segmentation and filtering rules, including onboarding of new services without weakening isolation.

Motorola Response

Comply.

We follow standardized SOPs for all segmentation changes:

- **Testing:** Proposed filtering rules are first validated in a test environment to ensure no impact on call routing.
 - **Onboarding:** New services are onboarded through a formal "Security Impact Analysis" that defines new VLANs and ACLs without weakening existing isolation.
 - **Validation:** Post-change, automated scans verify that only the intended ports are open.
-

- Monitoring & alerting for policy violation and lateral movement detection within/across segments, with procedures for rapid containment.

Motorola Response

Comply.

Our service provides continuous monitoring for policy violations and lateral movement detection.

- **Detection:** The system alerts on anomalies like "internal IP scanning" or "unauthorized inter-VLAN pings."
 - **Containment:** Upon detection of a violation, the NSOC initiates a rapid containment procedure, which may include automated port-shutdown or temporary isolation of the compromised segment via the BCF to prevent further spread across the ESInet.
-

4.2.4 Network Boundary Protection

Firewalls and Next Generation Firewalls (NGFWs) are key perimeter and inter-segment controls, but they are not the only defense. Internal systems must also be secure. The contractor must deploy a NENA-standard Border Control Function (BCF) or other boundary protections at all ESInet ingress/egress points and each segment entry/exit using explicit allow-lists that document required traffic and block all else. Specific BCF behaviors and requirements are identified in §E-2.1.1 of this document.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A boundary architecture showing boundary controls (BCF or NGFW) at all ESInet ingress and segment entry/exit. The BCF must conform to requirements in §E-2.1.1 of this document.

Motorola Response

Comply.

Our Boundary Architecture and BCF Conformance architecture places BCF and NGFW controls at every critical entry and exit point of the ESInet.

- **BCF Placement:** Standard-compliant BCFs (acting as SBCs with NG9-1-1-specific logic) are positioned at the OSP Ingress and at PSAP call handling system host egress points.
 - **Section E-2.1.1 Conformance:** Our BCF is purpose-built to meet the requirements of NENA-STA-010.3 and the specific mandates of §E-2.1.1. It performs:
 - **Admission Control:** Validating that all incoming SIP/RTP traffic originates from trusted, PCA-credentialed sources.
 - **DDoS/TDoS Mitigation:** Utilizing rate-limiting and behavioral analysis to block TDoS or volumetric attacks before they reach the ESRP.
 - **Media Anchoring:** Managing NAT traversal via ICE/STUN/TURN to ensure audio/video/text streams are established reliably.
-

- A traffic matrix for each firewall listing required services, ports, and protocols, with explicit allow rules; unnecessary traffic must be blocked by default.

Motorola Response

Comply.

Our firewall strategy is governed by an Explicit Allow policy. All traffic not explicitly defined in the matrix is blocked by default to minimize the attack surface.

Table 5-2: Firewall Strategy

Service Category	Ports / Protocols	Implementation Logic
SIP Signaling	TCP/UDP 5060, 5061 (mTLS)	BCF Policy-Enforced
Media (RTP/RTCP)	UDP 10000–20000	Dynamic Pinholing via SBC
Location (LoST)	TCP 443 (HTTPS)	ECRF/LVF Entry Point
Management	TCP 22 (SSH), 443 (HTTPS)	Restricted to OOB Mgmt VLAN
NTP / Monitoring	UDP 123, 161 (SNMP)	Hardened Core Services

- Performance & availability: high availability (HA) and/or failover capability, and traffic inspection features must be configured so boundary protections do not degrade service delivery capabilities.

Motorola Response

Comply.

To ensure that boundary protections do not introduce service degradation, our solution features:

- **High Availability (HA) & Failover:** All BCF and NGFW elements are deployed in Active-Active or Active-Standby clusters. If a primary gateway fails, the secondary node takes over stateful sessions (including active 911 calls) in sub-second timeframes, ensuring zero dropped calls.
- **Hardware-Accelerated Inspection:** Boundary devices utilize dedicated security processing units (SPUs) to perform deep packet inspection (DPI) on multimedia streams. This ensures that encryption (TLS 1.3) and threat filtering do not increase jitter or latency, maintaining audio and video quality for the telecommunicator.
- **Traffic Inspection Integrity:** While the BCF inspects headers for routing and security metadata, the payload remains protected. Our inspection features are tuned to prevent "false positives" that could block valid emergency traffic during high-volume events.

4.2.4.1 External Connections

NG911 relies on external connections; with these links often traversing the public internet, they must follow a zero-trust approach (NENA-STA-040.2 Appendix A & NIST Special Publication 800-207) and use layered protections. At minimum, each external connection must be protected by a boundary protection device conforming to requirements identified in §E-5.2.4 above, and any connection transporting sensitive information must use an encryption that conforms with the requirements identified in NENA-STA-040.2 §4.2.2.6 (Safeguarding Sensitive Electronic Information).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An external connectivity architecture listing counterparties, paths, and media, and how zero-trust principles are applied.

Motorola Response

Comply.

Our NGCS and ESInet employ a highly resilient, NENA i3-compliant architecture. Built on a defense-in-depth, zero-trust security model (NIST SP 800-53), it strictly controls how all external counterparties connect and exchange media with the core system.

Counterparties, Paths, and Media

- **Diverse Counterparties:** The system securely interconnects with OSPs, PSAPs, neighboring peer networks, and third-party data providers (e.g., LIS, ADR, TCCs).
- **Secure Connectivity Paths:** Traffic enters through geo-diverse Points of Interconnection (POIs) IP traffic via BCFs and legacy traffic via LNGs. Egress and inter-network routing utilize carrier-diverse, redundant MPLS networks with standardized NNI and UNI connections.
- **Standardized Media:** We support native Next Generation protocols, utilizing SIP for signaling, RTP for voice, MSRP for real-time text/SMS, and HTTP/HTTPS for secure data and location payloads (HELD, LoST, EIDO).

Application of Zero-Trust Principles

We enforce stringent security controls at every layer of the OSI model to ensure no counterparty, path, or media stream is implicitly trusted:

- **Strict Network Segmentation:** Stateful firewalls operate on a strict "deny-all" principle, isolating the PSAPs, ESInet, and NGCS into distinct security zones to prevent lateral movement.
 - **BCF:** SBCs normalize all incoming SIP traffic, hide internal network topologies, and automatically block abnormal or malicious patterns (such as TDoS attacks).
 - **End-to-End Encryption:** Data in transit is secured using TLS for SIP signaling, HTTPS for data queries, and FIPS 140-2 compliant IPsec with AES-256 encryption across the ESInet.
 - **Mutual Authentication:** System-to-system access requires strict mutual authentication, managed via Public Key Infrastructure (PKI) digital certificates issued by an approved PSAP Credentialing Authority (PCA).
 - **Least Privilege Access:** All user and vendor access is governed by RBAC and mandatory MFA.
-

- Evidence that all external links are protected by a firewall with placement, explicit allow-lists, and default-deny posture per §E-5.2.4.

Motorola Response

Comply.

Our service architecture employs strict firewall protections for all external links, fully aligning with best-practice requirements for strategic placement, default-deny postures, and explicit allow-listing.

- **Strategic Placement & Segmentation:** Firewalls are strategically deployed to create intentional logical boundaries between trusted and untrusted network zones, securely segregating production networks from DMZs. Every external connection—whether from outside entities or across different administrative domains—must pass through a firewall.
- **Default-Deny Posture:** To secure critical network assets and ensure malicious or unknown traffic is inherently rejected, every firewall across the solution operates on a strict "deny-all" foundation.
- **Explicit Allow-Lists:** Building on the default-deny posture, our firewalls actively inspect traversing traffic and utilize strict "allow-listing" (or "white-listing"). Only traffic that is explicitly authorized by predefined business, operational, and security rules is permitted to transit the network.

-
- An encryption approach for links carrying sensitive information, conforming to requirements of NENA-STA-040.2 §4.2.2.6, indicating where encryption is enforced.

Motorola Response

Comply.

Our service employs a rigorous encryption architecture to protect sensitive data both in transit and at rest. This approach strictly aligns with FIPS 140-2, NIST SP 800-53r4, and NENA security standards (NENA-STA-040.2).

Core Encryption Standards

- **AES-256:** The 256-bit Advanced Encryption Standard (AES) is utilized as the baseline for all encryption activities.
- **Data in Transit:** We employ TLS for external connections and SIP call signaling, IPsec and SDWAN overlay to ensure data confidentiality across the ESInet, and HTTPS for secure data queries and portal access.
- **Data at Rest:** All authentication credentials and passphrases are encrypted both during transmission and while stored.

Strict Enforcement Boundaries

Encryption is systematically enforced across multiple connection points to ensure zero-trust compliance:

- **The Network Edge & Interconnections:** SBCs enforce encryption at the ESInet edge to protect call flows and hide network topology, while AES-256 secures all interconnections between trusted and untrusted zones.
 - **Internal Segmentation:** Encryption is strictly mandated on all internal connections communicating between designated security zones.
 - **Remote Access:** All remote entry points require highly secure VPNs utilizing industry-standard encryption and Perfect Forward Secrecy (PFS).
-

- Operational controls for onboarding/approval, continuous monitoring, periodic review, and change/termination of external connections – consistent with zero-trust and boundary protection requirements.

Motorola Response

Comply.

We govern all external connections, including OSPs, third-party data providers, peer networks, and remote personnel, using a strict zero-trust and boundary protection architecture based on the NIST SP 800-53 framework. The entire lifecycle of external connections is securely managed through four operational phases:

- **Onboarding & Approval:** External integration begins with agency authorization (Letter of Agency). All new connections undergo rigorous ITIL-based Change Management, requiring Change Advisory Board (CAB) approval. Once approved, system-to-system access mandates strict mutual authentication via digital certificates.
 - **Boundary Protection & Monitoring:** External traffic is isolated using strict network segmentation. Traffic must pass through "deny-all" stateful firewalls (using explicit allow-lists) and SBCs to block malicious patterns. All connections are encrypted (TLS or IPsec AES-256) and monitored 24x7x365 by our NSOC utilizing advanced SIEM and IDS/IPS tools.
 - **Periodic Review & Audits:** To guarantee access remains restricted to authorized entities, all physical and logical ACLs and baseline security controls undergo mandatory quarterly reviews (true-ups). Boundary protections are further validated through annual independent audits (ISO 27001 and SOC 2 Type 2).
 - **Change & Termination (MACD):** Any modifications or terminations are managed through our ITIL Service Desk workflows. In strict compliance with NENA NG-SEC standards, we maintain rapid-response procedures to instantly revoke access, invalidate certificates for compromised or terminated entities, and securely decommission legacy network connections.
-

4.2.4.2 Demilitarized Zones (DMZ)

Some NG911 services must be reachable from untrusted networks. Any externally accessible resource not otherwise protected by equivalent controls must reside in a Demilitarized Zone (DMZ) that is segments from internal NGCS/ESInet segments and mediated by a boundary protection device per §E-5.2.4 of this document.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DMZ architecture showing externally accessible resources, segmentation from internal networks, and firewall/SBC/BCF demarcation points.

Motorola Response

Comply.

Our NGCS architecture employs a DMZ architecture with a defense-in-depth, zero-trust model to securely manage traffic and protect the core 9-1-1 routing engine.

- **DMZ for External Resources:** We utilize a secure DMZ to host externally accessible resources. This allows external sources to safely access the LVF and Web Portals without impacting live call routing (ECRF). All external portal access mandates MFA and continuous monitoring.
 - **Zero-Trust Segmentation:** Stateful firewalls strategically isolate internal production networks from the DMZ and untrusted domains. Operating on a strict "deny-all" posture, these firewalls use explicit allow-listing to permit only authorized traffic based on predefined business rules.
 - **BCF:** The BCF serves as the secure gateway for the ESInet, comprising redundant firewalls and SBCs. The firewalls provide primary network-level protection, while the SBCs act as Application Layer Gateways to normalize SIP traffic, hide internal topologies, and block malicious SIP activity.
 - **Strict Demarcation Points:**
 - **Ingress:** The inbound demarcation point is located at the POI, where OSP traffic, whether IP or legacy, enters securely behind the BCF.
 - **Egress (PSAP Boundary):** For traffic exiting the ESInet, the physical demarcation point is the LAN-facing port of our ESInet edge routers deployed at the PSAP call handling host facility, which securely connects to the CHE firewalls.
-

- A traffic controls strategy for the DMZ: default-deny posture, explicit allow lists, tightly limited ingress/egress, and no lateral access to internal segments.

Motorola Response

Comply.

We secure the DMZ and core internal networks through a strict zero-trust, defense-in-depth architecture. Our traffic control strategy relies on rigorous firewall policies and network segmentation to actively manage and protect data flows:

- **Default-Deny & Explicit Allow-Lists:** Firewalls segregating the DMZ from internal production networks and external domains operate on a strict "deny-all" principle. Only traffic explicitly authorized by predefined business and security rules (allow-listing) is permitted to transit.
 - **Tightly Governed Ingress & Egress:** We strategically deploy firewalls to create intentional logical boundaries between trusted, untrusted, and DMZ zones. All edge access is strictly controlled by the BCF, which pairs redundant firewalls with SBCs to filter packets and normalize all incoming SIP traffic before it enters the core.
 - **Prevention of Lateral Movement:** Our architecture utilizes rigorous network segmentation to isolate the DMZ, ESInet, PSAPs, and NGCS into distinct security zones. This stateful firewall-enforced separation ensures zero implicit trust, effectively blocking attackers from moving laterally into internal production systems if an externally accessible DMZ resource is ever compromised.
-

- Hardening & monitoring for DMZ assets: patch cadence, configuration baselines, centralized logging, telemetry, and alerting.

Motorola Response

Comply.

We apply rigorous security controls across our entire NGCS and ESInet architecture, ensuring all assets—including externally accessible resources in the DMZ—are highly protected, strictly maintained, and continuously monitored.

- **Configuration & System Hardening:** We utilize DISA STIGs as our primary system hardening framework. In compliance with NENA NG-SEC standards, systems enforce a zero-trust, "deny-all" posture and adhere to strict least-privilege principles to minimize the attack surface.
 - **Routine & Emergency Patch Management:** Operating systems are updated monthly and core networking systems quarterly, while anti-virus/malware definitions are applied in near real-time. Critical, time-sensitive security updates bypass standard schedules and are rapidly deployed via an expedited Emergency Change process.
 - **Centralized Logging & SIEM:** A NENA-compliant i3 Event Logger continuously aggregates data across all FEs. To ensure strict chain-of-custody auditability, all logs are GPS-time-synchronized via a NENA-compliant NTP master clock and fed directly into advanced SIEM tools for threat correlation.
 - **Telemetry & NSOC Alerting:** Our 24x7x365 NSOC utilizes active polling, passive collection, HIDS, and machine learning to detect anomalies. Breached thresholds automatically generate categorized trouble tickets and instantly dispatch alerts to designated stakeholders via email, SMS, or phone.
-

- Operational procedures for onboarding and retiring DMZ-hosted services, plus periodic reviews to confirm resources that require external access remain correctly isolated in the DMZ.

Motorola Response

Comply.

We govern the onboarding, retirement, and continuous isolation of DMZ-hosted services (such as the Location Validation Function) through a strict ITIL-based Change Management process and a zero-trust security framework.

- **Secure Onboarding:** The introduction of any new DMZ service or hardware begins with a formal service change request. After rigorous risk assessment by our Change Advisory Board (CAB) and Cybersecurity team, the service is deployed behind "deny-all" stateful firewalls using explicit allow-lists. An immediate out-of-band vulnerability scan is then conducted to verify the new asset's security posture and isolation.
 - **Systematic Retirement (MACD):** The decommissioning of services is strictly tracked through our Service Desk via Moves, Adds, Changes, and Deletions (MACD) workflows. We systematically retire associated network interfaces and transport links, and mandate the immediate revocation of all related access authority, credentials, and digital certificates.
 - **Rigorous Periodic Reviews:** To guarantee ongoing DMZ isolation and strict access control, our infrastructure undergoes a continuous and scheduled audit cadence:
 - **Quarterly Validations:** We conduct mandatory physical and logical ACL true-ups, alongside baseline security reviews. Any discovered deviations instantly trigger a Quarterly Risk Assessment Reporting (QRAR) workflow for immediate remediation.
 - **Annual Audits:** We perform comprehensive vulnerability scans and risk assessments structured around the NIST SP 800-30 standard. Our boundary protections are further validated through independent annual audits.
-

4.2.4.3 Defense in Depth

The contractor must apply Defense in Depth (DiD) – layered, overlapping controls that protect confidentiality, integrity, and availability across physical access, endpoints, data protection, boundary defenses, network and traffic separation, system monitoring, and (where applicable) vendor diversity. DiD ensures that if one control fails, others maintain security. Critical systems and sensitive information shall utilize Defense in Depth with deliberate redundancy and no single points of failure.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DiD architecture showing layered controls across the stack: physical access, endpoints, identity/authorization/authentication, boundary protections, and segmentation/traffic separation.

Motorola Response

Comply.

Our NG9-1-1 solution employs a robust, multi-layered DiD architecture based on the NIST SP 800-53 framework and NENA NG-SEC standards. Operating on a strict zero-trust model, we apply stringent security controls across every layer of the system:

- **Physical Access Controls:** Our facilities are secured 24/7/365 by guards, video surveillance, and biometric access. All system equipment is housed in locked cabinets, and sensitive infrastructure zones require strict two-factor authentication.
- **Endpoint & System Hardening:** To minimize the attack surface, devices and operating systems are rigorously hardened using DISA STIGs. We enforce the principle of least privilege, deploy advanced antivirus software, and maintain a continuous, strict patch management schedule.
- **Identity & Authentication:** Access is tightly restricted through RBAC and mandatory MFA for all remote and portal access. To ensure compliance, all physical and logical ACLs undergo mandatory quarterly true-ups.
- **Boundary Protections:** Our network perimeter actively filters traffic using redundant SBCs to normalize SIP traffic and block telephony attacks. Network boundaries are further fortified by Intrusion Detection and Prevention Systems (IDS/IPS) and active DDoS mitigation.
- **Segmentation & Traffic Separation:** We prevent lateral movement by deploying stateful firewalls that create strict logical boundaries between trusted production networks and untrusted DMZs.

These firewalls operate on a "deny-all" posture, permitting only explicitly allow-listed traffic. Furthermore, critical 9-1-1 voice traffic is prioritized using DSCP tagging, and all data is secured using AES-256, IPsec, and TLS encryption.

-
- A control-to-risk mapping for critical systems and sensitive data identifying how multiple independent controls address key threats, with no single-control dependencies.

Motorola Response

Comply.

We protect our service infrastructure and sensitive 9-1-1 data using a comprehensive, zero-trust Defense-in-Depth (DiD) strategy aligned with the NIST SP 800-53 framework. This overlapping architecture guarantees that no single security control is the sole point of failure.

We mitigate key threat vectors through the following layered, interdependent controls:

- **Unauthorized Access & Data Breaches:** We overlap strict physical facility security (24/7 guards, biometrics) with logical controls like RBAC and mandatory MFA. If a password is stolen, MFA blocks entry. If an insider attempts to overreach, RBAC limits their blast radius. Furthermore, end-to-end AES-256 and TLS encryption ensures any intercepted data remains entirely unreadable.

- **DDoS & TDoS Attacks:** We absorb volumetric IP attacks using multi-layer cloud scrubbing and firewall rate-limiting. If malicious traffic bypasses these perimeter limits, SBCs automatically drop malformed SIP packets. For sophisticated TDoS attacks, our core systems assign confidence levels to isolate suspected automated calls into dedicated queues, ensuring legitimate 9-1-1 emergencies are always answered.
 - **Malware & Ransomware:** All devices are rigorously hardened using DISA STIGs to minimize the attack surface, supported by 24/7 NSOC monitoring, Host-based Intrusion Detection (HIDS), and rapid patching. If a zero-day threat manages to bypass perimeter detection, strict "deny-all" network segmentation physically traps the infection within a single zone, completely neutralizing lateral movement.
 - **Critical Infrastructure Failure:** Our NGCS is built on a geo-diverse, multi-cloud microservices architecture backed by carrier-diverse MPLS networks and Tier 3 data centers (featuring redundant UPS and N+1 generators). If an entire physical region is destroyed by a disaster, our SDN fabric instantly and automatically steers traffic to healthy, geographically isolated cloud regions with zero loss of operational capacity.
-

- Failure mode and fallback analysis demonstrating how security is maintained if a layer is bypassed or fails.

Motorola Response

Comply.

Our service operates on a strict Defense-in-Depth (DiD) and zero-trust security model. Our architecture is explicitly engineered to eliminate single points of failure. If an attacker bypasses one control or a component fails, independent fallback layers instantly activate to contain the threat and maintain continuous 9-1-1 operations.

Here is how system integrity is maintained across five critical failure modes:

- **Identity Compromise:** If an attacker steals an authorized user's password via phishing, MFA blocks unauthorized portal or VPN access. Even if MFA were bypassed, strict RBAC enforces least-privilege access, severely limiting any potential impact.
- **Network Perimeter Intrusion:** If malware slips past external boundary defenses, strict network segmentation and "deny-all" stateful firewalls physically trap the threat within isolated zones (like a DMZ), preventing lateral movement. Simultaneously, internal HIDS and SIEM tools detect the anomaly and alert our 24x7x365 NSOC for immediate containment.
- **Telephony Denial of Service (TDoS):** If a massive wave of automated 9-1-1 spam bypasses network-level scrubbing, our SBCs automatically reject malformed SIP headers. If the spam calls are perfectly formed, our system uses directed queuing to isolate suspected automated calls into a dedicated queue, ensuring dispatchers can continue answering legitimate emergencies uninterrupted.
- **Call Routing / GIS Failure:** If primary geospatial routing fails due to missing or inaccurate local GIS data, the ECRF utilizes a hierarchical fallback routing safety net. The system automatically cascades from site structure address points to road centerlines, and ultimately to legacy MSAG/ESN or default routing, guaranteeing the call is delivered to a valid PSAP.

- **Critical Infrastructure Loss:** If a physical hardware component or entire facility experiences a service event, facility-level UPS and N+1 generators provide 24-to-36 hours of sustained power. If a region is entirely destroyed, our geo-diverse, multi-cloud microservices architecture (spanning at least three regions and two cloud providers) utilizes SDN for sub-second, automatic failover. Traffic is instantly steered to healthy regions with zero loss of system capacity.
-

- Operational integration with related sections (e.g., IAM/roles, segmentation, boundary protections, incident response, logging/monitoring), including runbooks for escalation between layers.

Motorola Response

Comply.

Our service employs a zero-trust, NIST SP 800-53 aligned architecture. Our system is designed so that security boundaries, identity management, monitoring tools, and incident response workflows operate as a continuous, automated feedback loop managed by our 24x7x365 NSOC.

Integrated Security & Monitoring Lifecycle

- **Boundary Sensors:** Strict network segmentation is enforced by stateful firewalls and SBCs. These edge devices act as the primary telemetry sensors for our monitoring layer.
- **Automated Threat Detection:** Telemetry is continuously fed into our i3 Event Logger, advanced SIEM tools, and HIDS. Any detected anomaly or unreachable probe automatically triggers a system alert.
- **ITSM Incident Generation:** Alerts are directly integrated into our ITSM platform (ServiceNow). The system automatically generates, categorizes (by severity), and presents actionable trouble tickets on NSOC dashboards.
- **Secure Visibility (IAM):** Authorized customer personnel can view real-time ticket status and system health via the CWP. Access is strictly governed by RBAC and MFA to ensure users only see data relevant to their jurisdiction.

SLA-Driven Escalation Runbooks

- When an incident is generated, the NSOC executes a strict, standardized runbook driven by event severity and SLA timers:
- **Prioritization & Notifications:** Tickets are immediately assigned a priority (Priority 1/Critical to Priority 4/Low). The ITSM instantly starts SLA timers and dispatches automated alerts (email, SMS, phone) to designated stakeholders.
- **Time-Based Escalation:** If an issue remains unresolved, it dynamically escalates based on support business processes.
- **Tiered Support Matrix:** Complex issues seamlessly escalate from Tier 1 (NSOC remote triage) to Tier 2 (NSOC Management), and finally to Tier 3 (Technical Support Organization and Service Delivery Leadership).

- **Critical Incident Bridges:** For Severity 1 and 2 incidents, the NSOC immediately initiates an Emergency Response Team bridge. This unites cybersecurity experts, core engineers, and field technicians, remaining active until a viable workaround or permanent resolution is fully implemented.
-

- Validation and review evidence and metrics showing layered control effectiveness over time.

Motorola Response

Comply.

We promote the ongoing effectiveness of its layered Defense-in-Depth (DiD) architecture through a rigorous combination of continuous telemetry, structured internal reviews, strict SLA tracking, and independent third-party audits.

- **Independent Third-Party Audits:** We provide objective, external validation of our operational security and availability through comprehensive Service Organization Controls (SOC 2 Type 2) reporting. Our frameworks system hardening is validated by DoD Joint Interoperability Test Command (JITC) Information Assurance certifications.
 - **Scheduled Internal Reviews:** Guided by the NIST SP 800-30 risk management framework, we systematically validate controls via Quarterly Risk Assessment Reporting (QRAR) and mandatory quarterly ACL true-ups. Out-of-band vulnerability scans are executed annually and immediately following any major system modifications.
 - **Strict SLA Performance Metrics:** The operational effectiveness of our redundant architecture is continuously measured against stringent SLAs, targeting 99.999% availability across the NGCS, ESInet, and Ingress points. We also track automated MOSs to guarantee voice quality remains at or above a 4.0 baseline. These metrics are transparently presented to the customer in monthly compliance reports.
 - **Continuous Monitoring & Root Cause Analysis:** Our 24x7x365 NSOC actively measures network behavior against historical trends utilizing advanced SIEM tools and HIDS. In the event of a control failure or outage, we conduct a formal Root Cause Analysis (RCA), generating an Event Analysis Report (EAR) to detail the timeline and implement long-term corrective actions.
-

4.2.4.4 Remote Access

Remote access connects users to systems outside a physical location. External remote access carries the highest risk and must be allowed only for documented business need, routed through authorized, secured, encrypted connections (e.g., VPN aligned to NIST SP 800-77), and enforced with strong authentication and centralized logging.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- **Access control & eligibility:** Processes ensuring external remote access is granted only for valid business need, with at least annual account reviews and timely removal when no longer required.

Motorola Response

Comply.

We manage external remote access, account eligibility, and credential lifecycles through a stringent zero-trust cybersecurity framework. We strictly enforce the principle of least privilege to ensure all access is securely provisioned, continuously audited, and rapidly revoked when no longer needed.

- **Strict Provisioning & Least Privilege:** Remote access is treated as a highly critical point of ingress and is continuously monitored by our 24x7x365 NSOC. Access is strictly limited to security-cleared, background-checked personnel. We enforce least privilege policies to ensure users are granted only the minimum permissions and rights necessary to perform their defined business roles.
- **Mandatory Quarterly Reviews:** Exceeding standard annual audit requirements, we conduct mandatory quarterly "true-ups" of all physical and logical ACLs. These rigorous routine audits verify that only current, authorized users with an ongoing operational need retain their access rights.
- **Rapid Revocation & Termination:** In strict compliance with NENA NG-SEC standards, we maintain documented procedures to immediately revoke access authority, credentials, and digital certificates for terminated or compromised personnel. Furthermore, external agency access to customer portals is promptly deauthorized and removed upon written notification from the customer.

-
- **Secure connectivity:** Use of an authorized, encrypted connection for all external remote access. MFA must be implemented for all remote connectivity.

Motorola Response

Comply.

We guarantee the security of all external and remote connections through a tightly controlled, zero-trust framework that strictly mandates encryption and MFA across all access points.

- **Mandatory MFA:** Strict MFA is required for all remote network access, including external user interfaces, system dashboards, and reporting portals.
- **Advanced VPN Encryption:** All remote sessions are facilitated through highly secure VPNs utilizing AES-256 encryption, Perfect Forward Secrecy (PFS), and ephemeral keys to ensure absolute data confidentiality in transit.
- **Continuous NSOC Monitoring:** We treat remote access as a highly critical point of ingress. All sessions are actively monitored in real-time by our 24x7x365 NSOC, and access is exclusively limited to security-cleared, background-checked personnel.

- **Physical Endpoint Security:** The physical hardware and network facilities where these VPN connections terminate are additionally secured by strict, physical two-factor authentication controls.
-

- Operational governance: SOPs for requesting, approving, establishing, and terminating remote access, plus periodic tests/reviews to confirm controls remain effective.

Motorola Response

Comply.

We manage the operational governance of remote access through a rigorous zero-trust cybersecurity framework, strictly aligning with NENA NG-SEC and NIST SP 800-53 standards. Our end-to-end lifecycle ensures that all remote access is securely provisioned, actively monitored, and continuously audited.

- **Strict Provisioning & Least Privilege:** All remote access requests require formal documentation and explicit Security Administration approval. Eligibility is strictly limited to cleared, background-checked personnel. We enforce the principle of least privilege, ensuring users are granted only the minimum permissions necessary for their specific roles.
 - **Secure Connectivity & Monitoring:** Remote sessions mandate MFA and are facilitated via AES-256 encrypted VPNs utilizing Perfect Forward Secrecy (PFS). We enforce stringent credential policies (e.g., 15-character minimums, 180-day expirations), and all remote ingress is actively monitored in real time by our NSOC.
 - **Rapid Access Revocation:** We maintain documented SOPs for the immediate revocation of access, credentials, and digital certificates for terminated personnel or compromised accounts. External agency portal access is promptly deauthorized upon written customer notification.
 - **Continuous Auditing & Testing:** To validate control effectiveness over time, we mandate quarterly physical and logical ACL "true-ups" and baseline security reviews. We actively test network integrity through routine out-of-band vulnerability scanning, and our overarching governance is verified annually.
-

- Logging & monitoring: centralized logging for remote connectivity in conformance with minimum requirements identified in NENA-STA-040.2 §6.17.

Motorola Response

Comply.

Our NGCS and ESInet solutions deliver robust, centralized logging and continuous monitoring capabilities that strictly comply with NENA management standards (NENA-INF-040.2 / NENA-STA-040.2).

We ensure full visibility, auditability, and threat detection across all remote connectivity through the following integrated controls:

- **Centralized Logging & SIEM Integration:** Our NENA-compliant i3 Event Logger securely aggregates transaction logs and metadata across the entire architecture 24x7x365. This data is fed into advanced SIEM tools, allowing our NSOC to correlate network traffic, system events, and security alerts to rapidly identify potential threats.
 - **Remote Connectivity Tracking:** All remote access points—which strictly mandate MFA and encrypted VPNs—are actively controlled and monitored in real time. Boundary devices, including stateful firewalls and HIDS, meticulously log network behavior. Additionally, all remote troubleshooting and service events are formally tracked as tickets within our ITSM system (ServiceNow).
 - **Auditability & Tamper-Proof Integrity:** To guarantee legal defensibility and strict chain-of-custody, every logged event is accurately timestamped down to the millisecond using a GPS-synchronized, NENA-compliant NTP hardware master clock. These logs are securely stored and protected against tampering, ensuring they remain highly available for incident analysis and independent auditing.
-

4.2.5 Infrastructure Resilience

Mission-critical NG911 functions must remain available despite single-component failures and localized outages. The contractor must employ redundancy and diversity across the ESInet and NGCS, through the deployment of high-availability mechanisms with supported infrastructure where appropriate. Because infrastructure failures can drop in-progress sessions, applications and signaling must gracefully recover during a path or site failure. NGCS/ESInet components must be both redundant and diverse, and ingress traffic must enter the NG911 system through diverse paths. (Additional redundancy guidance in NENA-STA-010.3 §2.9).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An end-to-end High Availability (HA) architecture showing redundant components and physically diverse ingress/egress, transport, facilities, and power; include call/signaling paths proving diverse 911 call entry.

Motorola Response

Comply.

Our services are engineered to support 99.999% operational availability. Our end-to-end High Availability (HA) architecture is meticulously designed to eliminate all single points of failure across hardware, software, facilities, and network transport.

Facilities & Power Infrastructure

- **Geo-Diverse Cloud Data Centers:** Core routing elements are housed in highly secure facilities meeting Tier 3 (Thermal) and Tier 4 (Power) standards, physically hardened against EF5-category winds.
- **Robust Power Redundancy:** Equipment is supported by redundant A/B Power Distribution Units (PDUs), 2N UPS systems (providing 15-minute runtime at 80% load), and N+1 independent generators capable of sustaining operations at 100% load for at least 36 hours.

Transport & Egress (ESInet)

- **Carrier & Physical Diversity:** The ESInet utilizes carrier-diverse MPLS and Broadband networks and physically diverse routing/building entrances to prevent localized physical damage or carrier-specific cyberattacks from disrupting service.
- **Sub-Second Convergence:** Utilizing dynamic routing protocols (OSPF, BGP) and Fast Reroute (FRR) technologies, the network detects link failures and automatically steers traffic to healthy paths in under 54 milliseconds.

NGCS Core Components

- **Multi-Cloud Redundancy:** The core routing intelligence operates across at least three geographically diverse regions (East, Central, West US) utilizing at least two major cloud providers to ensure non-correlated statistical reliability.
- **Microservices & SDN:** Core FEs utilize a microservices architecture. If a single instance fails, the SDN instantly isolates it and steers traffic to healthy Availability Zones without impacting peer services.

Call Ingress & Intelligent Routing Path

- **Redundant Ingress (POIs):** OSP traffic enters through load-balanced, geo-diverse Points of Interconnection (POIs). Legacy TDM calls are distributed across redundant LNGs, while SIP traffic is normalized and secured by the BCF.
- **Resilient Call Delivery:** Once safely ingressed, signaling and location data traverse redundant IP links to the ESRP. The ESRP queries the ECRF (location) and PRF (policy/availability) before seamlessly routing the call out over diverse ESInet links to the PSAP. From the OSP handoff to the delivery of the call to the host call handling system, every component has an active, automated backup.

-
- Component-level HA designs with health checks, failover criteria, and state synchronization.

Motorola Response

Comply.

Our services deliver a resilient, 99.999% operational available architecture with zero single points of failure. Our system ensures seamless continuity through containerized microservices, active telemetry, automated sub-second failovers, and real-time state synchronization.

Distributed Component Redundancy

- **Core Microservices:** Critical elements (ESRP, PRF, ECRF, LVF) operate in an Active/Active configuration across geographically diverse, multi-cloud regions. If one instance degrades, peer microservices instantly absorb the workload without interrupting live calls.

- **Edge & Gateway Redundancy:** BCF (SBCs/firewalls) and LNGs are deployed in fully redundant pairs to distribute load and prevent capacity loss.
- **PSAP Call Handling:** Edge equipment (SD-WAN routers) utilize redundant Active/Active or Active/Standby configurations to guarantee no active calls are dropped during a major fault switchover.

Continuous Health Telemetry

- **Active NSOC Probes:** Predictive monitoring continuously polls all network elements. Unreachable probes automatically trigger failovers and generate ITSM trouble tickets.
- **SIP Heartbeats:** SIP OPTIONS messages continuously verify the health and availability of endpoints and peering networks.
- **Network Detection:** Dynamic routing protocols (BGP, OSPF) paired with Bidirectional Forwarding Detection (BFD) provide sub-second IP node fault detection.

Automated Failover Execution

- **Sub-Second Convergence:** During a transport link failure, Fast Reroute (FRR) technologies steer traffic to healthy, redundant paths in under 54 milliseconds.
- **Component Switchover:** Hardware or software degradation mandate immediate failover to a redundant component
- **Policy-Driven Routing:** The PRF instantly intercepts SIP errors (e.g., 486 Busy) or Ring-No-Answer (RNA) timeouts, immediately pulling the call back to apply alternate overflow routing rules.

Active State Synchronization

- **Database Replication:** SI publishes GIS updates to a master database, which utilizes SQL replication to sync child ECRF/LVF databases in near real-time. This ensures data is synchronized without impacting live call-routing performance.
- **Location & GIS Sync:** Bidirectional web services actively synchronize the LDB with GIS data, ensuring failover routing relies on perfectly matched state data.
- **VM Snapshots & Backups:** Active/Active environments continuously sync state, backed by rigorous grandfather-father-son backup schemes and pre/post-change VM snapshots for instant configuration restoration.

-
- A diversity plan detailing route/provider diversity, facility/region separation, and power diversity.

Motorola Response

Comply.

Our service architecture guarantees 99.999% availability through a strictly engineered diversity plan. This approach systematically eliminates single points of failure across all network pathways, physical/cloud facilities, and power systems.

- **Route & Provider Diversity:** Carrier & Path Independence: We leverage multiple national MPLS carriers and Broadband carriers using physically diverse "last-mile" routing and building entrances, where available, to prevent localized physical damage or single-carrier cyberattacks from disrupting service.
 - **Diverse Ingress:** OSP traffic is distributed across load-balanced, geographically diverse Points of Interconnection (POIs).
 - **Automated Convergence:** Utilizing SDN and dynamic routing protocols (OSPF, BGP, BFD), the network automatically detects broken routes and steers traffic to redundant paths in under 54 milliseconds, with zero loss of live audio.
 - **Facility & Region Separation:** Multi-Cloud Architecture: Core NGCS elements are distributed across at least three distinct US regions (East, Central, West) utilizing at least two major cloud providers. This ensures outages in one region or provider are statistically non-correlated with the others.
 - **Physical Hardening:** Physical data centers housing core aggregation sites meet a minimum of Uptime Institute Tier 3 standards and are structurally hardened to withstand EF5-category winds (up to 318 mph).
 - **Power Diversity:** A/B Power & UPS Backup: All hardware is connected to isolated A/B Power Distribution Units (PDUs), backed by a 2N UPS architecture providing at least 15 minutes of immediate runtime at 80% load in our data center facilities.
 - **Prolonged Generator Resiliency:** N+1 independent generators automatically activate within 60 seconds of utility instability, sustaining operations for 24 to 36 hours at 100% load.
 - **Fueling Contracts:** Facilities maintain dedicated, SLA-backed local fueling contracts (e.g., 1-to-4-hour response times) to ensure continuous operation during extended regional disasters.
-

- Application/session continuity methods that demonstrate graceful recovery during device/site failover.

Motorola Response

Comply.

Our NGCS and ESInet architecture guarantee application and session continuity during component or network failures. We achieve graceful recovery and uninterrupted 9-1-1 operations through sub-second network convergence, active/active microservices, and rigorous active-call testing.

- **Sub-Second Network Convergence:** Our transport layer utilizes dynamic routing (OSPF, BGP) paired with Bidirectional Forwarding Detection (BFD) and Fast Reroute (FRR) technologies. This ensures the network detects failures and automatically reroutes traffic in under 54 milliseconds, preventing any loss of active RTP audio streams or SIP signaling.
- **Active/Active Microservices:** NGCS FEs are encapsulated within microservice clusters distributed across multiple cloud Availability Zones. If an instance fails, peer microservices instantly absorb the workload.
- **SIP & Media (RTP) Recovery:** To maintain sessions during degraded conditions, we utilize SIP session keep-alives (RFC 4028). If an element detects a loss of RTP media (audio), the system automatically triggers a re-INVITE with a "Target Refresh," allowing a healthy element to take over the dialog and restore the media session gracefully rather than tearing down the call.

- **Proven "Brute Force" Testing:** We mandate ultimate proof of graceful recovery during PSAP Final Acceptance Testing (ATP). While live test calls with two-way audio are actively in progress, hardware elements and circuits are intentionally failed using "brute force" methods (e.g., physically unplugging cables). The strict passing metric dictates that there must be no loss of two-way audio for longer than 2 seconds during any failure scenario.
-

- Testing & exercise evidence for failover/fallback, with measured recovery objectives and tracked corrective actions.

Motorola Response

Comply.

Our service architecture provides seamless application and session continuity. We validate our 99.999% availability and failover mechanisms through stringent active-call testing, strict recovery objectives, and highly tracked corrective action workflows.

Application & Session Continuity

- **Sub-Second Convergence:** Our transport layer utilizes dynamic routing (OSPF, BGP) and Fast Reroute (FRR) to automatically bypass network failures in under 54 milliseconds, ensuring zero loss of SIP signaling or active routing.
- **Non-Disruptive Microservices:** Core elements operate in Active/Active microservice clusters. If an instance fails, peer microservices instantly absorb the workload.
- **SIP/RTP Graceful Recovery:** To maintain sessions during degraded conditions, we utilize SIP keep-alives (RFC 4028). If an element detects a loss of RTP (audio) media, the system triggers a "Target Refresh" re-INVITE, gracefully shifting the dialog to a healthy element rather than tearing down the call.

Rigorous Testing & Measured Objectives

- **Failover ATP:** During PSAP Final Acceptance Testing (ATP), failover is tested under live conditions. We mandate that hardware and circuits be intentionally failed using physical disconnections while live 9-1-1 test calls are in progress.
- **Strict Continuity Metrics:** During testing, our strict passing criterion dictates no loss of two-way audio for longer than 2 seconds.
- **30-Day Reliability Test:** Post-cutover, the system undergoes a continuous 30-day live reliability test. Any critical routing failure stops the clock, forces a correction, and completely resets the 30-day testing period.
- **Defined RTOs/RPOs:** Our formal DR/BC plans mandate regular exercises and explicitly define Recovery Time and RPOs for all critical data.

Tracked Corrective Actions

When a test fails or an operational incident occurs, we utilize strict ITIL-based tracking systems to ensure rapid, verified resolution:

- **Project Punch Lists & Registers:** During implementation, defects and risks are actively tracked via Issue Logs and real-time Punch Lists, requiring formal dual sign-off from both Motorola and the customer before final acceptance.

- **Root Cause Analysis (RCA):** For any service-affecting failure, we generate a preliminary report within 3–5 days, followed by a comprehensive Event Analysis Report (EAR) detailing the timeline, root cause, and preventative actions within 10 to 30 days.
 - **Post-Implementation Reviews (PIR):** All corrective network changes undergo a PIR to feed our continuous problem management cycle, reducing the future frequency and impact of incidents.
-

- Operations & monitoring for infrastructure health; maintenance procedures that avoid creating single points of failure during changes, and SOPs for failure scenarios.

Motorola Response

Comply.

Our service employs a highly structured, ITIL-based operational framework managed by our NSOC. This ensures continuous health monitoring, seamless zero-downtime maintenance, and rapid, standardized responses to any system failures.

Infrastructure Health & Continuous Monitoring

- **Automated Telemetry & ITSM:** Advanced NMS actively poll all network devices and FEs. Breached thresholds automatically generate categorized trouble tickets within our ITSM platform (ServiceNow) for immediate NSOC triage.
- **Real-Time Visibility:** Authorized agency personnel access a secure CWP featuring a "Situational Awareness" dashboard to visually monitor real-time node status, call routing activity, and capacity utilization.

Maintenance Procedures (Zero Single Points of Failure)

- **Independent Servicing:** Our Active/Active, geo-diverse architecture allows technicians to take one side of the system completely offline for maintenance while the redundant side seamlessly processes 100% of live call capacity without dropping traffic.
- **Strict Change Management:** All maintenance requires a formal service change request to assess risk and impact, including a minimum 10-day customer notice for all non-emergency changes.
- **Mandatory Rollbacks & Snapshots:** Every approved change is accompanied by a documented rollback plan. Virtual Machine (VM) snapshots are taken immediately prior to execution, guaranteeing instant restoration to a pre-change state if unexpected issues arise.

SOPs for Failures

- **Classification & Emergency Response:** Failures are classified across four severity levels. Priority 1 (Critical) incidents trigger a 15-minute response target, hourly stakeholder updates, and the immediate launch of an Emergency Response Team (ERT) bridge that remains active until a resolution is implemented.
- **SLA-Driven Escalation:** Unresolved issues automatically escalate based on elapsed SLA target times (50% to the assigned engineer, 75% to the Engineering manager, 100% to the Senior Manager of Technical Service Delivery).

- **Automated Fallback Routing:** If a PSAP or network fails, the PRF instantly applies pre-configured Overflow, Busy, or Alternate/Abandonment routing rules to ensure continuous call delivery.
 - **Post-Incident Analysis:** Following the restoration of a major failure, we provide a preliminary Reason for Outage (RFO) report within 3 to 5 days, followed by a final Root Cause Analysis (RCA) detailing exact causes and long-term preventative actions within 30 days.
-

4.3 Authentication and Federated SSO

Agent authentication across NG911 must use federated Single Sign-On (SSO) based on OASIS SAML v2.0. Identity Providers (IdPs) authenticate agents and issues assertions to Relying Parties (RPs) for authorization. For HTTP-bound apps, IdPs and RPs must support Web Browser SSO, Identity Provider Discovery, and Single Logout; ECP and Artifact Resolution may be supported. SAML metadata should be aggregated under one `<EntitiesDescriptor>` and digitally signed by an identified administrative body using a well-known certificate to bootstrap trust.

Motorola Response

Comply.

For session establishment between agents and elements, SSO authenticates the agent and unlocks the agent's private key; the agent's X.509 certificate is then used to form the TLS session. For SIP and HTTPS, mutual TLS (mTLS) must be used with certificates traceable to the PCA for agents, agencies, and elements. RSA-2048 must be supported and accepted and accepted ESInet-wide (alternatives may be accepted only if cryptographically equivalent to, or stronger than RSA-2048). Each IdP must enforce multifactor authentication (MFA) for agents using a combination of at least two (additional factors preferred) of the following: password, token, smart card, or biometrics. Offline or other locally available backup authentication methods should be implemented for use if network access to primary authentication methods is unavailable.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An SSO architecture showing IdP(s), RPs, and assertion flows; conform all agent operations requiring authorization rely on SAML v2.0.

Motorola Response

Comply.

We propose a centralized, SAML v2.0-compliant Single Sign-On (SSO) architecture to secure all agent operations requiring authorization across the NGCS and ESInet. This federated approach ensures centralized identity control, consistent authorization enforcement, and full interoperability with your existing IAM systems.

- **Centralized Identity Provider (IdP):** Authentication is driven by either the Motorola Advanced Identity Cloud or a seamlessly integrated, customer-approved IdP. The IdP serves as the authoritative source for user authentication and MFA policy enforcement.
 - **Service Providers (Relying Parties):** All FEs, ECRF and administrative portals act as Relying Parties (RPs). They inherently trust the central IdP and do not perform any local authentication.
 - **Secure Assertion Flows:** We fully support SP-initiated flows utilizing HTTPS, XML signatures, and certificate-based trust. Upon successful IdP login, signed SAML v2.0 assertions are sent to the RP's Assertion Consumer Service (ACS) to establish the authenticated session.
 - **Strict Authorization Control:** All authorization-sensitive operations (such as call taking, database provisioning, and security administration) rely exclusively on these validated SAML assertions. The assertions are strictly time-bound, audience-restricted, and deliver the user identity and role attributes necessary for RPs to enforce precise access control.
-

- mTLS designs for SIP and HTTPS using PCA-traceable certificates for agents, agencies, and elements; include trust anchors, path validation, and revocation checks.

Motorola Response

Comply.

Our NG9-1-1 architecture secures all core communications and data exchanges through a rigorous Public Key Infrastructure (PKI) framework, utilizing mutual TLS (mTLS), PCA-traceable certificates, and strict real-time validation mechanisms.

- **Mutual TLS (mTLS) for SIP & HTTPS:** We mandate mTLS to secure all traffic. SIP over TLS (SIPS) utilizes mutual authentication to establish firewall-like security for call signaling and media streams between endpoints. Additionally, all PSAP data queries (HELD, LoST, ADR) are secured via encrypted HTTPS/TLS. All connections enforce Perfect Forward Secrecy (PFS) to proactively protect past sessions against future key compromises.
- **PCA-Traceable Trust Anchors:** All NGCS functional elements carry valid identity certificates signed by a Certificate Authority (CA). The system fully supports roles authenticated directly by the NIOC PCA. Until the National PCA is fully deployed, we serve as the regional PCA utilizing an RSA 2048-based ICA, which acts as the interim trust anchor and is designed to be cross-signed with the National PCA upon its release.
- **Strict Path Validation & Revocation:** Our VESTA NXT Router Service and interconnecting elements actively enforce continuous certificate validity to ensure the chain of trust remains intact. Automated validation checks include:
 - **Path & Signature Validation:** Verifying the CA signature and complete chain of trust.
 - **Identity Validation:** Confirming the validity of the certificate's "distinguished name" within the x.500 database.
 - **Expiration & CRL Checks:** Enforcing authorized validity periods and actively querying CRLs to immediately reject expired or revoked certificates.

- **Compromise Protocols:** We maintain documented, rapid-response procedures for key holders to instantly initiate revocation if private keys are suspected of compromise.
-

- A cryptographic baseline confirming RSA-2048 support and acceptance ESInet-wide and policy for accepting alternatives only if equivalent to, or stronger than RSA-2048.

Motorola Response

Comply.

Our proposed solution provides a robust cryptographic baseline across the architecture, strictly enforcing standardized encryption protocols and active RSA-2048 support.

Our architecture mandates the following cryptographic controls to secure data at rest and in transit:

- **RSA-2048 & PCA Integration:** We operate a regional PSAP Credentialing Authority (PCA) utilizing an RSA-2048-based certificate authority. Combined with mandatory two-factor authentication, this guarantees unauthorized devices cannot access the ESInet. Our PCA is fully compatible with the NIOC PCA and is architected for seamless cross-signing upon the national registry's full deployment.
 - **AES-256 & FIPS Compliance:** Our solution utilizes AES-256 for encryption. All access points and internal communications mandate cryptographic modules that strictly adhere to NIST FIPS 140-2 and FIPS 140-3 standards.
 - **Secure Transport (TLS) & PFS:** All external connections require secure HTTPS/TLS. Furthermore, all key exchange algorithms must support Perfect Forward Secrecy (PFS) to proactively protect past data sessions against any future key compromises.
 - **Standardized Adherence:** We rely exclusively on standardized protocols and reputable vendors, ensuring all private keys are strictly safeguarded. While our baseline is firmly rooted in RSA-2048, any cryptographic capability utilized within the system must meet validated NIST standards and remain in full compliance with stringent NENA NG-SEC guidelines.
-

- IdP MFA enforcement: supported factors, enrollment of multiple factors, and backup local authentication.

Motorola Response

Comply.

We mandate a strict MFA framework to secure all remote, external, and privileged access. Enforced centrally, this zero-trust approach ensures robust identity verification and uninterrupted service continuity.

- **Mandatory MFA Enforcement:** MFA is strictly required for all remote access, VPN connections, and external interfaces (including the CWP, PRF portal, and system dashboards), as well as all mission-critical and privileged accounts.
- **Centralized IdP Governance:** A centralized Identity Provider (IdP) governs all authentication decisions, ensuring MFA policies are consistently enforced prior to granting any authenticated session, regardless of the user's network location or access method.

- **Diverse Authentication Factors:** To guarantee access resilience, the IdP supports multiple enrolled factors. Users authenticate via combinations of knowledge factors (PINs, passphrases), possession factors (RSA SecurID tokens, X.509 certificates), and cryptographic device credentials.
 - **Cryptographic Foundation:** Our authentication architecture leverages an RSA 2048-bit certificate authority combined with two-factor authentication to protect credentials and explicitly block unauthorized devices.
 - **Secure Continuity & Backup:** To maintain operational continuity during an IdP outage, we provide strictly controlled, fully audited backup local authentication that remains in full alignment with your overarching security policies.
-

- The TLS establishment flow where SSO authentication unlocks the agent's private key used with the agent's certificate to negotiate the TLS session.

Motorola Response

Comply.

Our proposed solution implements a highly secure, SSO-gated mutual TLS (mTLS) architecture. This approach ensures a strict cryptographic binding between user identity, device identity, and encrypted backend communications.

- **Encrypted Key Storage:** Each agent is provisioned with a unique X.509 certificate issued by a trusted RSA 2048-bit Certificate Authority. The associated private key is securely encrypted on the device and remains completely inaccessible until successful authentication.
 - **SSO-Gated Unlocking:** Authentication is performed via an approved Identity Provider (IdP) that enforces enterprise policies, including MFA and role validation. Upon successful SSO authentication, the agent's private key is temporarily unlocked within a protected keystore exclusively for the duration of the active session.
 - **mTLS Negotiation:** The agent utilizes its certificate and temporarily unlocked private key to perform standard mTLS handshakes with backend services, actively validating server identity, client trust, and key ownership.
 - **Session Termination Re-Locking:** The moment a session ends or the user logs out, the private key is immediately re-locked. It cannot be reused to establish connections without initiating a full SSO reauthentication.
-

- Operational controls: onboarding/offboarding, key & certificate lifecycle, assertion & metadata signing key rotation, and monitoring/logging of authentication events.

Motorola Response

Comply.

We enforce strict operational controls to securely manage user access lifecycles, cryptographic assets, and continuous authentication monitoring.

- **User Lifecycle Management (Onboarding/Offboarding):** We maintain formal, documented procedures for the entire user access lifecycle. All new accounts and resource authorizations require explicit documentation and security administration approval. Upon any role change or termination, documented procedures dictate the immediate modification or complete revocation of access.
 - **Cryptographic Key & Certificate Lifecycle:** All cryptographic keys and digital certificates are subject to strict, end-to-end lifecycle management:
 - **Strict Safeguarding:** Employees are mandated to safeguard and never share private encryption keys.
 - **Continuous Validation:** Certificates undergo continuous validity testing, verifying the CA signature, authorized validity periods, identity accuracy, and active CRL status.
 - **Rapid Revocation:** We enforce formal, immediate revocation protocols if a key holder suspects a private key or digital certificate has been compromised.
 - **Continuous Monitoring & Logging:** Authentication events are actively controlled and audited to prevent unauthorized access:
 - **24x7x365 NSOC & SIEM:** Our Operations Center continuously correlates system logs and security alerts in real time using advanced SIEM tools.
 - **Automated Access Restrictions:** The system actively restricts unauthorized access, automatically locking out users after a maximum of five invalid sign-on attempts.
 - **Granular Audit Reporting:** All actioned events are logged in our ITSM system. Following any service-impacting issue, we can provide highly detailed physical and virtual access reports down to the individual device level.
-

4.4 Cryptography and Public Key Infrastructure

Cryptography in NG911 primarily secures connections and proves identity: asymmetric keys/X.509 certificates authenticate endpoints and establish sessions; symmetric ciphers then protect data in transit. The NG911 PKI is PCA-rooted: the PSAP Credentialing Agency (PCA) issues subordinate CA certificates to ESInet-operated Intermediate CAs (ICAs). Approved ICAs may, in turn, issue end-entity certificates to NGCS/ESInet service elements, and personnel. Full controlling specifications for the NG911 PKI are: NG911 Interoperability Oversight Commission (NIOC) PSAP Credentialing Agency Certificate Policy, and NIOC PSAP Credentialing Agency Certificate Validation Policy.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- PKI trust architecture showing the PCA root, Contractor-operated ICA(s), end-entity certificate issuance, and provision for subordinate ICA implementation and certificate issuance.

Motorola Response

Comply.

We secure the NG9-1-1 environment through a robust Public Key Infrastructure (PKI) trust architecture. Our solution seamlessly integrates a National PCA root, a Contractor-operated ICA, and flexible provisions for subordinate CAs and end-entity issuance.

- **National PCA Integration:** We fully support and integrate with the NIOC PSAP Credentialing Authority (PCA), utilizing direct or cross-signed certificates for all NGCS operations and interoperability.
 - **Our-Operated Regional ICA:** Until the National or State authority is fully established, we operate a highly secure, RSA 2048-based ICA to act as your regional PCA. This ICA is explicitly designed for seamless compatibility and cross-signing with the National PCA upon its deployment.
 - **Flexible Subordinate CAs:** Our architecture supports cross-signing and integration with state-level or national-level CAs. We can establish dedicated subordinate intermediate CAs, utilizing unique, registered domain names to guarantee an unbroken chain of trust.
 - **End-Entity Issuance & Demarcation:** All NGCS FEs carry valid identity certificates traceable to a public source of trust. While we provision and maintain all certificates required for NGCS-to-PSAP interconnections, local PSAPs retain full control and responsibility over their internal, non-NGCS certificates (e.g., CAD, internal Windows systems).
-

- Operational practices for certificate lifecycle and key management, including how asymmetric authentication bootstraps TLS/mTLS and how symmetric session keys are negotiated.

Motorola Response

Comply.

We strictly govern the lifecycle of all cryptographic assets, ensuring digital certificates remain valid, private keys are fiercely protected, and all session negotiations utilize state-of-the-art encryption protocols.

- **Continuous Certificate Validation:** We actively evaluate digital certificates by verifying the CA signature, matching the current date against the authorized validity period, and validating the identity's "distinguished name." The system continuously queries CRLs to immediately reject any revoked or expired certificates.
- **NGCS Certificate Maintenance:** We provision and maintain all certificates technically required for NGCS interconnections, ensuring they trace back to a public source of trust, an ICA, or the National PCA. (Note: Exact issuance, deployment, and renewal workflows are collaboratively tailored and finalized during the project implementation phase).

- **Strict Key Management & Revocation:** Personnel are mandated to safeguard encryption keys and are strictly prohibited from sharing private keys. We enforce formal, immediate revocation protocols if a key holder suspects a compromise, or when formally required during personnel changes (e.g., termination or investigation).
 - **TLS/mTLS & Perfect Forward Secrecy (PFS):** To secure external communications, we utilize TLS for hop-by-hop authentication and integrity protection. All SIP traffic is mandated to use SIPS (SIP over mTLS) utilizing CA-signed certificates for mutual authentication. Furthermore, all remote access and TLS key exchanges utilize ephemeral keys and support Perfect Forward Secrecy (PFS) to permanently protect past sessions against any future key compromises.
-

- Certificate profiles & example chains demonstrating path validation to the PCA, with revocation checking and trust-anchor management.

Motorola Response

Comply.

Motorola acts as the regional PSAP Credentialing Authority (PCA) until a state or national authority (such as the NIOC/National PCA) is established, at which point they will coordinate and integrate with the established authority.

Here is how PCA certificate management and revocation checking work within the system:

Certificate Management and PKI Architecture

- **Certificate Authorities (CA):** Motorola operates its own ICA, which supports cross-signing with state or national level CAs. The Public Key Infrastructure (PKI) design utilizes two independent public Root CAs (VESTA R1 and VESTA R2) that issue the Intermediate CAs.
- **Cross-Certification:** To achieve redundancy, Intermediate CAs are cross-certified (cross-signed). This means they are issued a certificate from both root CAs, providing two paths to resolution. If there is an issue resolving the chain of trust down one path, the system experiences no downtime.
- **Secure Key Storage:** Private key passwords for all CAs are stored securely in a Thycotic Secret Server vault. The passwords are only available to authorized CA Administrators and are randomized by the server once checked back in.
- **Expiration and Notifications:** Certificates have strict lifespans: Root CAs expire in 9 years, Intermediate CAs in 5 years, Server Certificates in 1 year, and Client Certificates in 90 days. Automated tools monitor these expiration dates and send escalating email notifications to the associated points of contact as the expiration date approaches.
- **Rollover Process:** To ensure seamless transitions, a rollover process is utilized where multiple CAs run side-by-side. Before a CA expires, expiring server and client certificates are renewed using a newly generated Intermediate CA. An issued certificate's expiration date must never exceed its issuing CA's expiration date.

Revocation Checking: The system continuously checks certificate validity to ensure expired or compromised digital certificates are not used. This is handled through the following mechanisms:

- **CRL and OCSP Services:** A dedicated certificate management server provides revocation query services via CRL and the Online Certificate Status Protocol (OCSP).

- **Server Distribution:** There are four revocation servers placed within each PSAC (two in a public-facing DMZ and two in the internal network). The actual revocation is executed on the issuing servers, which then push the updated CRL files to the revocation servers via SSH.
- **Client Queries:** Information regarding revocation is embedded directly into the v3 extensions section of all x.509 certificates. The applications using these certificates are responsible for querying the specified URIs (over HTTP) to confirm the certificate has not been revoked.
- **Local Caching:** To guarantee high availability, systems implement a local cache of revocation data. This allows path discovery and certificate validation to continue even if the system temporarily loses network access to the primary revocation servers.

The following is a sample certificate chain from an existing Motorola NGCS deployment which is leveraging a PCA as its root of trust.

Device certificate:

Common Name: ecrfab.ng911.telus.ca

Subject Alternative Names: ecrfab.ng911.telus.ca, ecrf.ng911.telus.ca, IP Address:75.156.201.19, othername:elementid/ecrfab.ng911.telus.ca/ECRF/ng911.telus.ca

Organization: TELUS Communications Inc.

Organization Unit: ECRF Alberta

Locality: Vancouver

State: British Columbia

Country: CA

Valid From: February 20, 2024

Valid To: March 17, 2026

Issuer: TELUS ICA2, TELUS Corporation

Serial Number: 2c0c9a37a3216966043fa9e1b6cd7b7d7fb0d1ee

Intermediate certificate:

Common Name: TELUS ICA2

Subject Alternative Names: othername:<unsupported>

Organization: TELUS Corporation

Organization Unit: ICA2-0001

Locality: Vancouver

State: British Columbia

Country: CA

Valid From: March 15, 2022

Valid To: March 15, 2032

Issuer: TELUS CPCA Root CA, TELUS Corporation

Serial Number: 51930561626244 (0x2f3b06adc084)

Root certificate:

Common Name: TELUS CPCA Root CA

Subject Alternative Names: othername:<unsupported>

Organization: TELUS Corporation

Organization Unit: Root CA-1

Locality:

State:

Country: CA

Valid From: March 15, 2022

Valid To: March 15, 2042

Issuer: TELUS CPCA Root CA, TELUS Corporation

Serial Number: 3917653946751 (0x390265f317f)

-
- Conformance statements confirming acceptance of PCA-rooted RSA-compatible credentials, consistent with the controlling specifications from the NIOC PCA Certificate Policy and NIOC PCA Certificate Validation Policy.

Motorola Response

Comply.

We provide explicit conformance to NIOC standards for the acceptance, validation, and management of PCA-rooted credentials.

- **Formal NIOC Compliance:** We fully comply with the NIOC V1.0.0 PCA Certification Validation Guidelines, ensuring the secure validation and issuance of certificates across the NG9-1-1 Public Key Infrastructure.
- **Acquisition & Role Authentication:** Our core routing services natively authenticate roles using NIOC PCA certificates. The system is fully equipped to seamlessly acquire and validate credentials from any NIOC PCA-vetted ICA.
- **Endpoint Utilization:** We commit to utilizing NIOC/National PCA-issued certificates—or Motorola certificates cross-signed by the NIOC—at all endpoints required for NGCS operations and interoperability.

- **RSA-2048 Interim Trust Anchor:** Until the NIOC PCA is fully implemented, we act as a regional PCA utilizing a highly secure RSA 2048-based certificate authority. Combined with strict two-factor authentication to block unauthorized access, this interim trust anchor is explicitly designed to be cross-signed with the National PCA the moment it is deployed.
-

- **TLS alignment:** where and how TLS/mTLS is enforced across NGCS/ESInet interfaces showing asymmetric establishment and symmetric protection in session.

Motorola Response

Comply.

We strictly enforce TLS and mutual TLS (mTLS) across our NGCS and ESInet architecture. This zero-trust framework leverages asymmetric cryptography for secure session establishment and symmetric cryptography for high-speed data payload protection.

Strict Enforcement Boundaries

- **SIP Signaling (SIPS):** Mutual authentication is explicitly required for all network-to-network interfaces (NNIs) with peer providers and OSPs using TLS-encrypted channels.
- **Edge Security:** SBCs act as back-to-back proxies at the network edge, providing TLS termination and firewall-like security for SIP signaling and incoming media streams.
- **PSAP Data Queries:** Secure HTTPS/TLS connections are strictly mandated between the provider network and PSAP CHE for all HELD, LoST, and ADR requests.
- **WAN Connections:** All traffic traversing the PSAP Local Area Network (LAN) to the ESInet Wide Area Network (WAN) is secured via encrypted TCP/IP connections.

Cryptographic Mechanisms

- **Asymmetric Session Establishment:** To securely negotiate session keys, we utilize X.509 digital certificates signed by the National or Regional PCA, grounded in an RSA-2048 trust anchor. We mandate Perfect Forward Secrecy (PFS) utilizing ephemeral keys to guarantee that past sessions remain entirely secure even if a long-term private key is compromised in the future.
 - **Symmetric Payload Protection:** Once the asymmetric handshake successfully authenticates the endpoints, the session instantly transitions to 256-bit Advanced Encryption Standard (AES) to rapidly encrypt the actual data payload. All sensitive data in transit is protected with FIPS 140-2 compliant AES-256 and IPsec protocols, providing robust hop-by-hop integrity.
-

4.4.1 Cryptographic Keys

Cryptographic keys underpin identity and data protection in NG911. Keys are algorithm-specific and generated by approved processes. For asymmetric key pairs, the public key is submitted to a CA for inclusion in an X.509 certificate and the private key is securely stored. Private and symmetric keys must be protected against loss, corruption, and unauthorized access, with periodic access reviews. Private keys should be classified as 'Sensitive (Most Sensitive Information)' in alignment with NENA-STA-040.2 §4.2.2.1.4, or at a comparable level that aligns with the contractor's existing data classification schema.

Private keys must be revoked and reissued if compromised, or if compromised is suspected. Cryptographic key implementations must adhere to the NIOC PCA Certificate Policy and NIOC PCA Validation Policy and align with the NENA i3 Standard (NENA-STA-010.3) and NIST SP 800-57 Part 2 Rev. 1 (Recommendation for Key Management: Part 2: Best Practices for Key Management Organizations).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Key generation & issuance procedures: how keys are generated, how public keys are submitted to the CA, and where/how private keys are stored.

Motorola Response

Comply.

We enforce a rigorous, standards-based approach to cryptographic key generation, storage, and personnel safeguarding to ensure absolute protection of all private keys and sensitive data.

- **Standardized Key Generation:** Cryptographic keys are generated utilizing approved algorithms and key sizes on secure user devices, servers, or HSMs. All modules protecting sensitive data strictly comply with NIST FIPS 140-2 and FIPS 140-3 requirements.
 - **Secure Certificate Issuance:** Public keys are packaged into Certificate Signing Requests (CSRs) and securely transmitted to the Certificate Authority (CA) for validation and issuance within our RSA 2048-based CA trust hierarchy.
 - **Strict Private Key Isolation:** Private keys are never shared with the CA. They remain securely isolated on the system where they were generated, preferably within an HSM or encrypted keystore, and are protected by strong authentication and restricted access controls.
 - **Rigorous Personnel Safeguards:** We maintain strict operational policies regarding key access. Personnel are expressly prohibited from sharing private encryption keys with anyone, except under formally documented, authorized, and approved procedures.
-

- A classification statement designating private keys as 'Sensitive (Most Sensitive Information),' or similar, and the technical/administrative controls that enforce this classification.

Motorola Response

Comply.

We enforce a rigorous, standards-based framework to guarantee the absolute protection of all private keys and sensitive data. We formally classify private cryptographic keys as "Sensitive" (Most Sensitive

Information) due to their critical role in authentication and trust enforcement, mandating the highest level of technical and administrative protection across the environment.

We enforce this classification through the following rigorous lifecycle controls:

- **Standardized Key Generation:** Keys are generated utilizing approved algorithms and sizes on secure user devices, servers, or HSMs. All modules protecting sensitive data strictly adhere to NIST FIPS 140-2 and FIPS 140-3 requirements.
 - **Secure Certificate Issuance:** Public keys are packaged into Certificate Signing Requests (CSRs) and securely transmitted to the Certificate Authority (CA) for validation and issuance within our RSA 2048-based trust hierarchy.
 - **Strict Private Key Isolation:** Private keys are never shared with the CA. They remain securely isolated on the system of generation—strictly within an HSM or encrypted keystore—and are fortified by strong authentication and restricted access controls.
 - **Rigorous Administrative Safeguards:** We mandate uncompromising operational policies regarding key access. Personnel are expressly prohibited from sharing private encryption keys with anyone, except under formally documented, authorized, and strictly approved exception procedures.
-
- Access control & periodic review: who/what can access keys, authentication required, separation of duties, and the cadence/mechanics of access recertification.

Motorola Response

Comply.

We govern access to the service through stringent administrative controls, enforcing the principle of least privilege, zero-trust authentication protocols, and continuous lifecycle management.

- **Least Privilege & Key Safeguarding:** Physical and logical access is restricted strictly to authorized personnel only based on their specific roles. Employees are mandated to safeguard assigned encryption keys and are expressly prohibited from sharing them, except under formally documented administrative demands (e.g., investigations or terminations).
 - **Strict Authentication & MFA:** MFA is mandatory for all remote access, mission-critical accounts, and external portals. We enforce unique user IDs (no shared accounts), a 5-attempt lockout threshold, and stringent password policies (12-character minimum, 90-day expiration). To prevent single-incident compromise, authentication factors must be stored separately.
 - **Separation of Duties (SoD):** To guarantee strict segregation of duties and prevent unauthorized modifications, developers are explicitly prohibited from serving as System Administrators for the production environments they create.
 - **Quarterly Access Recertification:** We mandate quarterly logical and physical ACL "true-ups" to verify that only active, authorized personnel retain access. Formal lifecycle management procedures dictate the immediate modification or complete revocation of access upon any role change or termination.
-
- Key protection measures for storage/backup/restore, including protections at rest and in use, and configuration practices consistent with current TLS guidance.

Motorola Response

Comply.

Our proposed solution provides stringent cryptographic measures across our Next Generation 9-1-1 (NG9-1-1) and ESInet architecture, ensuring absolute security for sensitive data and credentials at rest, in transit, and during backup/restore operations.

Data & Credential Protection (At Rest & In Use)

- **AES-256 & FIPS Compliance:** All sensitive data is encrypted at rest and in transit utilizing AES-256 encryption, fully complying with FIPS 140-2 and NIST SP 800-53r4 standards.
- **Strict Credential Storage:** Authentication credentials must be securely encrypted. Passwords and passphrases cannot be stored in function keys or hardcoded into scripts without explicit business justification and heavy compensating controls (e.g., encryption and workstation locks).
- **MFA Factor Separation:** To prevent a single security incident from compromising an account, the architecture mandates that MFA components (e.g., Certificate + Passphrase) are never stored together.
- **Key Safeguarding:** Employees are strictly mandated to safeguard assigned encryption keys. Sharing private keys is expressly prohibited, with exceptions strictly limited to formal administrative demands (e.g., investigations).

Secure Backup & Restore Operations

- **Formal Backup Rotation:** We actively maintain system backups across all servers utilizing a secure grandfather-father-son rotation scheme, with additional backups triggered automatically during any system configuration change.
- **Tactical VM Snapshots:** To provide immediate rollback capabilities, Virtual Machine (VM) snapshots are captured immediately before and after change events. These serve as rapid tactical restorations complementing the formal, secure backup schedule.

TLS Configuration & Fallback Practices

- **SIPS & Perfect Forward Secrecy (PFS):** Mutual authentication via CA-signed certificates is required for SIP over TLS (SIPS). Crucially, all TLS key exchange algorithms mandate Perfect Forward Secrecy (PFS), guaranteeing that past session keys remain secure even if a long-term private key is breached in the future.
- **Encrypted PSAP Queries:** Secure HTTPS/TLS connections are strictly mandated between the provider network and the CHE for all critical data queries (HELD, LoST, ADR).
- **Session Management & Resiliency:** TCP/TLS is the preferred transport protocol, engineered to securely reuse TLS connections for SIP responses within the same dialog. If a TLS connection fails, the system automatically re-establishes it utilizing SIP headers or DNS SRV records. To prioritize life-safety, the system will seamlessly fall back to UDP if negotiated by an upstream system, ensuring the 9-1-1 call continues processing without dropping.

-
- A compromise response plan detailing detection, revocation, re-issuance, distribution, and restoration steps when keys are, or suspected to be, compromised

Motorola Response

Comply.

We comply with NENA NG-SEC standards for managing compromised cryptographic keys and digital certificates. We maintain a rigorous, end-to-end framework for the rapid detection, revocation, and restoration of compromised credentials to ensure absolute system integrity.

- **Detection & Suspicion:**
 - **Automated Validity Testing:** Systems continuously verify Certificate Authority (CA) signatures, authorized date ranges, and distinguished names.
 - **Mandatory Reporting:** Key holders are strictly required to immediately initiate formal revocation protocols the moment they suspect their private key has been compromised.
 - **Rapid Revocation Enforcement:**
 - **Formal Procedures:** We enforce formal, immediate revocation procedures for compromised digital certificates.
 - **Active CRL Verification:** The CHE and core routing elements actively query CRLs during validity testing to instantly identify and block revoked certificates.
 - **NSOC Incident Response & Restoration:** If a key compromise is tied to a broader cyberattack, our 24x7x365 Network Security Operations Center (NSOC) executes a strict incident response plan consisting of:
 - **Containment:** Isolating unauthorized access to prevent lateral movement or further damage.
 - **Eradication:** Removing any malware or malicious code facilitating the compromise.
 - **Restoration & Analysis:** Restoring affected systems to full functionality, followed by a comprehensive post-incident root-cause analysis to implement preventative security measures.
 - **Re-Issuance & Distribution:** Operational controls dictate that all digital certificates must be kept current, and systems will strictly reject any expired or invalid certificates. (Note: Exact certificate re-issuance, deployment, and renewal workflows are collaboratively tailored and finalized during the implementation phase).
-

- Lifecycle management covering creation, distribution, rotation, archival and destruction, with logging/audit trails sufficient for compliance and forensics.

Motorola Response

Comply.

Our NG9-1-1 and ESInet solution integrates rigorous cryptographic lifecycle management with tamper-proof logging mechanisms. Our architecture is meticulously engineered to support legal forensics, strict chain-of-custody, and comprehensive compliance audits.

Key & Certificate Lifecycle Management

- **Creation & Rotation:** Cryptographic elements utilize standard protocols under a PKI/PCA/ICA framework. Automated validity testing actively rejects expired or invalid certificates, while user passwords enforce strict, mathematically defined expiration intervals (e.g., 30 to 90 days).

- **Active Revocation:** The system continuously queries CRLs. Additionally, key holders are strictly mandated to initiate immediate revocation protocols if a private key compromise is even suspected.
- **NIST-Compliant Archival & Destruction:** At service termination, customer data and cryptographic material can be returned, securely removed, or permanently destroyed by Motorola in strict accordance with NIST SP 800-88 "Media Sanitization Guidelines." Following permanent destruction, we provide a formal, legally binding "Certificate of Destruction."

Logging, Forensics, and Compliance

- **Tamper-Proof Chain of Custody:** Our NGCS i3 Event Logger operates as a highly secure transaction logger. It is explicitly designed to prevent record tampering and preserve a legally verifiable chain of custody, ensuring all logged 9-1-1 records and metadata remain eligible as evidence in court proceedings.
 - **Comprehensive Security Logging:** The system securely aggregates and stores granular logs of all critical system events, CDRs, network traffic behavior, and security alerts.
 - **Compliance & Retention:** Our open-records compliant logging architecture adheres strictly to CJIS Security Policy and NIST SP 800-53 requirements. It easily supports customized, long-term data retention schedules based on your specific agency requirements.
 - **Independent Auditing:** To consistently prove compliance and operational security, Motorola undergoes rigorous, independent third-party audits, maintaining active SSAE 18 SOC 2 Type 2 and ISO 27001 certifications.
-

- Conformance attestations to the NIOC PCA Certificate Policy and NIOC PCA Validation Policy.

Motorola Response

Comply.

Our proposed solution conforms to the NIOC standards for the acceptance, validation, and management of PCA-rooted credentials across our NGCS.

- **Formal NIOC Compliance:** We fully comply with the NIOC V1.0.0 PCA Certification Validation Guidelines, ensuring the secure validation and issuance of certificates across the NG9-1-1 Public Key Infrastructure.
 - **Acquisition & Role Authentication:** Our core routing services natively authenticate roles using NIOC PCA certificates. The system actively acquires and validates credentials from any NIOC PCA-vetted ICA.
 - **Endpoint Utilization:** We commit to utilizing NIOC/National PCA-issued certificates, or Motorola certificates cross-signed by the NIOC, at all endpoints required for NGCS operations and interoperability.
 - **Interim Trust Anchor & Future Cross-Signing:** Until the NIOC PCA is fully implemented, we act as a regional PCA utilizing a highly secure RSA 2048-based certificate authority. Combined with strict two-factor authentication to block unauthorized access, this interim trust anchor is designed to be cross-signed with the National PCA the moment it is deployed.
-

4.4.2 Use of Self-Signed Certificates

Self-signed certificates MUST NOT be used for any NG911 communications that traverse an ESInet. All communications must use certificates traceable to the PCA root. External entities that are not in the PCA-traceable PKI must present certificated issued by a reputable public Certificate Authority. This ensures peer identity is validated through a recognized trust chain and prevents unauthenticated endpoints from participating in NG911 exchanges.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A certificate policy and enforcement plan affirming no self-signed certificates within or between ESInets and that NGCS/PSAP elements use PCA-anchored certificates.

Motorola Response

Comply.

Our proposed service security policies prohibit the use of self-signed certificates. We mandate the use of traceable, Certificate Authority (CA)-signed credentials to ensure absolute cryptographic trust across all secure network operations.

- **Prohibition of Self-Signed Certificates:** All SIP messaging must traverse a TLS-encrypted channel (SIPS). We strictly mandate mutual authentication for these connections utilizing exclusively CA-signed certificates issued by a PCA or an authorized third-party CA.
 - **PCA-Anchored Traceability:** All NGCS components and FEs carry valid identity certificates traceable to a public source of trust. Motorola provisions and maintains all certificates required for NGCS-to-PSAP interconnections, utilizing registered, unique domain names to guarantee an unbroken chain of trust.
 - **NIOC Integration & Interim RSA-2048 ICA:** We formally commit to utilizing NIOC) PCA-issued (or cross-signed) certificates at all endpoints. Until the National PCA is fully established, Motorola acts as your regional PCA via our own RSA 2048-based ICA, which is explicitly architected for seamless cross-signing once the national registry is deployed.
 - **Continuous Automated Enforcement:** Our architecture continuously enforces this trusted certificate policy through automated validity testing. The system actively verifies CA signatures, enforces authorized validity date ranges, confirms the x.500 "distinguished name" identity, and continuously queries CRLs to instantly reject any revoked, expired, or self-signed certificates.
-

- External entity onboarding requirements stating non-PCA participants must use Public CA certificates, and how this is verified during trust establishment.

Motorola Response

Comply.

We enforce mutual authentication and trust establishment protocols for all external entities connecting to our service. We integrate with OSPs and peer networks while maintaining an uncompromising, zero-trust cryptographic boundary.

- **Mandatory CA-Signed Certificates:** All external interconnections must utilize SIPS (SIP over TLS) with mutual authentication, managed securely by our edge SBCs. We strictly require that all presented certificates be CA-signed, issued either by the PCA or an explicitly authorized third-party CA.
 - **Streamlined Onboarding (NNI):** To facilitate secure and efficient integration, we provide comprehensive Network-to-Network Interface (NNI) control documents detailing the exact APIs, minimum requirements, and standards-based security policies external systems need to interoperate with the network.
 - **Automated Trust Verification:** During session establishment, the VESTA NXT Router Service and connecting elements execute a rigorous, automated validity testing process:
 - **Signature Validation:** Mathematically validates the CA signature to confirm the unbroken chain of trust to the PCA or third-party CA.
 - **Validity Period:** Verifies the current date falls within the certificate's authorized, active lifespan.
 - **Identity Verification:** Validates the x.500 "distinguished name" to guarantee the certificate exactly matches the connecting entity.
 - **Revocation Checks:** Actively queries CRLs to instantly reject any revoked credentials prior to expiration.
-
- Trust store and path-validation configuration for SIP, HTTPS, APIs, and management interfaces, accepting only PCA-anchored chains (or approved public CA chains) with CRL/OSCP checks.

Motorola Response

Comply.

Our service supports TLS, PCA-anchored credentials, and rigorous path validation across all SIP, HTTPS, API, and management interfaces to guarantee zero-trust communication.

- **Interface Security (SIP, HTTPS, APIs):** All SIP signaling utilizes SIPS (SIP over TLS) governed by edge SBCs for firewall-like security. We strictly mandate encrypted HTTPS/TLS for all PSAP CHE connections and critical API queries (HELD, LoST, ADR).
- **Management & Portal Access:** All external management interfaces, system dashboards, PRF portals, and database maintenance portals strictly enforce MFA.
- **Trust Stores & PCA-Anchored Chains:** Mutual authentication requires CA-signed certificates issued by a PCA or an authorized third-party CA. All NGCS elements carry identity certificates traceable to a public trust source, Motorola's ICA, or the NIOC PCA. We fully commit to utilizing NIOC-issued or cross-signed certificates at all required NGCS endpoints.

- **Automated Path Validation & Revocation:** Our VESTA NXT Router Service and all connecting elements continuously execute an automated validity testing workflow during session establishment:
 - **Signature Validation:** Mathematically validates the CA signature to ensure an unbroken chain of trust.
 - **Validity Period:** Verifies the current date falls within the authorized active lifespan.
 - **Identity Verification:** Validates the x.500 "distinguished name" to guarantee identity authenticity.
 - **Active CRL Checks:** Continuously queries CRLs to instantly reject any revoked credentials.
 - An asset/certificate inventory and automated detection controls to identify and block self-signed or untrusted certs.
-

Motorola Response

Comply.

We enforce cryptographic controls to automatically identify and block self-signed or untrusted certificates, paired with rigorous, end-to-end operational management of all cryptographic assets.

- **Prohibition & Automated Blocking:** We strictly prohibit the use of self-signed credentials. All SIPS connections mandate mutual authentication utilizing certificates issued exclusively by a PCA or an authorized third-party CA. Our systems actively block untrusted access via continuous, automated validity testing that verifies:
 - **CA Signatures:** Mathematically validates the signature to guarantee the certificate stems from a trusted root and is not self-signed.
 - **Active Revocation (CRL):** Continuously queries CRLs to instantly reject any compromised credentials.
 - **Validity Periods:** Confirms the current date falls strictly within the authorized active lifespan.
 - **Identity Verification:** Validates the x.500 "distinguished name" to authenticate the exact connecting entity.
 - **Inventory & Lifecycle Governance:** Motorola assumes direct operational responsibility for the comprehensive inventory and lifecycle management of these cryptographic assets across the environment.
 - **End-to-End Management:** We create, provision, and maintain all certificates required for NGCS FEs and PSAP interconnections.
 - **Traceable Trust:** Every managed certificate carries a valid identity explicitly traceable back to a public source of trust, our ICA, or the National PCA.
 - **Continuous Auditing:** We maintain strict logical access controls and conduct regular baseline validations—including comprehensive Quarterly Risk Assessment Reporting—to ensure continuous compliance, identify exceptions, and proactively manage security controls.
-

- An exception policy confirming there are no exceptions for self-signed certificates on ESInet-traversing communication, including test and non-production environments.

Motorola Response

Comply.

Our proposed solution supports a zero-exception policy regarding cryptographic trust: self-signed certificates are strictly prohibited for any ESInet-traversing communication. This unwavering standard applies universally across all environments, including production, development, and testing.

- **Universal CA-Signed Mandate:** All ESInet communications, specifically those utilizing SIPS (SIP over TLS), mandate mutual authentication using certificates issued exclusively by a trusted PCA or an authorized third-party Certificate Authority (CA).
 - **Production-Parity Test Environments:** Our lab and test environments are deployed as cloud-native instantiations of the live call routing service. Because they exactly simulate the production core, they adhere to the same stringent Network-to-Network (NNI) and User-to-Network (UNI) interface security standards, inherently blocking any self-signed credentials.
 - **Standardized Implementations:** All cryptographic deployments mandate standard security applications, protocols, and formats, and must be sourced exclusively from reputable, vetted vendors rather than relying on proprietary or self-signed cryptology.
-

4.5 Integrity Protection

All NG 911 protocol operations must be integrity-protected with TLS, using SHA-256 or stronger (FIPS PUB 180-4); SHA-256 must be supported by all implementations. These controls make messages and media tamper-evident end-to-end.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An integrity protection design confirming TLS deployment on all NGCS/ESInet protocol exchanges with SHA-256, and network-wide support for SHA-256.

Motorola Response

Comply.

Our proposed solution supports AES-256 encryption, TLS, and SHA-256 hashing across all NGCS and ESInet protocol exchanges to guarantee absolute data confidentiality and message integrity. Weaker cryptographic algorithms are strictly prohibited across the network.

- **AES-256 & FIPS Compliance:** All sensitive data (both at rest and in transit) and internal inter-component communications (via IPSec) are secured using 256-bit Advanced Encryption Standard (AES-256). This strategy fully complies with NIST FIPS 140-2 and FIPS 140-3 validated cryptographic standards.
 - **SHA-256 Hashing Mandate:** All TLS configurations require cryptographic cipher suites that utilize SHA-256 for hashing and message integrity.
 - **SIP Signaling (SIPS) & Resiliency:** Network-to-network SIP messages utilize SIPS (SIP over TLS) with mandatory mutual authentication. Key exchange algorithms must support Perfect Forward Secrecy (PFS). To prioritize life-safety, the system will seamlessly fall back to UDP if negotiated by an upstream system, ensuring the 9-1-1 call never drops.
 - **Encrypted PSAP Queries:** Secure HTTPS/TLS connections are strictly mandated between the NGCS network and PSAP CHE for all critical data queries, including HELD, LoST, and ADR requests.
-

- Cipher/algorithm policy and configuration artifacts proving acceptance of SHA-256 and procedures to prevent/detect downgrades.

Motorola Response

Comply.

We support a robust cryptographic baseline, mandating SHA-256 (or stronger) and AES-256 encryption while proactively prohibiting legacy algorithms to eliminate the risk of downgrade attacks.

Encryption & Cryptographic Baselines

- **Approved Algorithms:** We mandate SHA-256 (or stronger) and strictly prohibit legacy hashes such as SHA-1 and MD5. All sensitive data at rest and in transit is protected using 256-bit Advanced Encryption Standard (AES-256).
- **FIPS Compliance:** All cryptographic modules and security systems operate in full compliance with NIST FIPS 140-2 and FIPS 140-3 validated standards.
- **Standardized Implementations:** We exclusively utilize standardized, reputable vendor implementations, actively enforcing IPSec with AES-256 for all inter-component communications.

Downgrade Prevention & Zero-Trust Architecture

- **Protocol & Cipher Enforcement:** We inherently prevent downgrade attacks by explicitly disabling legacy protocols, enforcing strict cipher ordering, and validating secure configuration baselines.
- **TLS & Perfect Forward Secrecy (PFS):** All external connections utilize TLS for hop-by-hop authentication. SIPS connections strictly require key exchange algorithms that support Perfect Forward Secrecy (PFS).
- **Zero-Trust Boundaries:** Firewalls establish a logical discontinuity between network zones, operating on a strict "deny-all" posture that permits only explicitly authorized protocols.

Continuous Monitoring & Vulnerability Detection

- **24x7x365 NSOC & Machine Learning:** Our NSOC utilizes advanced SIEM tools and IDS/IPS empowered by machine learning to continuously detect anomalous traffic patterns or protocol manipulations.
 - **Automated Certificate Validation:** Systems continuously validate CA signatures and actively query CRLs to ensure secure handshakes are never compromised by invalid credentials.
 - **Proactive Scanning:** We execute rigorous vulnerability scans on a regular schedule—and immediately following any major system change—to continuously validate our security posture.
-

- Verification & monitoring: evidence that interfaces negotiate required integrity algorithms; ongoing checks to prevent regression.

Motorola Response

Comply.

We verify and monitor all applicable interfaces that securely negotiate required integrity algorithms through controlled configuration baselines, rigorous validation testing, and continuous monitoring to actively prevent security regression.

Interface Negotiation Standards

- **TLS & Perfect Forward Secrecy (PFS):** All interfaces secure call signaling and media streams utilizing TLS, explicitly mandating that key exchange algorithms support Perfect Forward Secrecy (PFS).
- **SIP & SDP Negotiation:** TLS connections are established using parameters advertised within ingressing SIP headers (e.g., Via or Contact). For media streams, Session Description Protocol (SDP) negotiation strictly dictates parameters such as DTMF handling.
- **Strict Codec Compliance:** To ensure voice quality and interoperability, interfaces mandate the G.711 codec with a 20ms packetization rate, strictly prohibiting the use of silence suppression.

Verification & Regression Prevention

- **Continuous Baseline Validation:** We systematically review baseline controls to prevent security degradation, culminating in a formal Quarterly Risk Assessment Report (QRAR) that evaluates all deployment-specific controls and exceptions.
 - **Mandatory Regression Testing:** Our NG9-1-1 integration process features a strict "Defect Tracking & Resolution" phase. Any implemented fix or Emergency Change Request automatically triggers a mandatory rescan and revalidation to ensure the security posture has not regressed.
 - **Active Integrity Monitoring:** Our 24x7x365 Network Security Operations Center (NSOC) deploys active network probes across the ESInet to monitor system health. Additionally, elements receiving calls are continuously polled via SIP OPTIONS on a per-URI basis to verify connection integrity and routing capabilities during periods of inactivity.
-

- Exception handling for legacy interoperability (where deployed), with compensating controls and a timeline to reach full SHA-256 compliance.

Motorola Response

Comply.

We provide a risk management framework to support legacy interoperability exceptions in environments where strict modern cryptographic standards (such as SHA-256) are not yet natively feasible. We secure these environments using transitional architecture and robust compensating controls while actively driving a documented migration plan toward full Next Generation 9-1-1 (NG9-1-1) compliance.

Transitional Architecture & Compensating Controls

- **Legacy Gateways:** To bridge non-IP environments, we deploy specialized LNG, LSRGs, and LPG.
- **Strict Border Control & Segmentation:** All legacy traffic is forced through our BCF and SBCs. This ensures strict network segmentation, edge security normalization, and continuous audit logging before any traffic enters the ESInet.
- **Protocol & Data Conversion:** Legacy TDM circuits and ALI data are actively converted into secure SIP protocols and i3-compliant CLDXF payloads via specialized Protocol, Location, and MSAG Interworking Functions (PIF, LIF, MCS).
- **Hierarchical Fallback Routing:** If legacy location data lacks geospatial confidence, the ECRF automatically enforces a safety net by falling back to tabular MSAG or Emergency Service Number (ESN) routing.
- **Active Exception Management:** Legacy data integrity issues (e.g., "No Record Found" or misroutes) are actively captured, tracked, and resolved via our web-based Discrepancy Reporting Service (DRS).

Path to Full Compliance

- **Documented Migration Plans:** We provide a formal migration plan with defined milestones to achieve full IP/SIP and cryptographic compliance, based on your system inventory and operational constraints.
- **Aggressive Project Timelines:** Our standard project scope targets the migration of all legacy OSP connections to native IP/SIP within 120 days of the NGCS "go-live" date.
- **Regulatory Alignment:** Our timelines align with the FCC Report and Order (FCC 24-78), which mandates OSP transitions from TDM to SIP and location-based routing within 6 to 24 months, effectively forcing the retirement of vulnerable LNGs.

4.5.1 JSON Web Signatures (JWS)

The contractor must implement JWS exactly as specified in the NENA i3 Standard (NENA-STA-010.3 §5.10), including, but not limited to, serialization, algorithm, discovery, certificate/chain handling, and Logging Service provisions defined therein. This RFP does not restate i3's normative details; Respondents must conform to i3 requirements as currently defined.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A statement of conformance to JWS requirements of NENA-STA-010.3 §5.10, plus a clause-by-clause matrix mapping the implementation to each i3 requirement.

Motorola Response

Comply.

We conform to the JWS standard regarding the strict NENA i3 JWS implementation requirements, while JWS integration for the Policy Store is actively scheduled on our product roadmap for a future release.

- JWS uses Flat JSON serialization format
- JWS uses EdDSA as the signature method
- JWS Protected Header contains exactly one “alg” field
- LogEvents supports both unsigned (“alg” set to “none”) and signed JWS
- **Policy Store (Roadmap Deviation):** Currently, our system does not format all routing and access policies as a signed JWS. The strict NENA requirement for the Policy Store to save, retrieve, and cryptographically verify byte-for-byte JWS documents by the ESRP prior to executing routing rules is actively on our engineering roadmap
- **Current Compensating Controls:** In the interim, while JWS Policy Store functionality is in development, all routing rules and access policies are strictly protected against unauthorized alteration through our centralized RBAC and Zero Trust architectural boundaries.

- Operational policies reflecting i3 requirements and certificate/chain handling with long-term stability where applicable.

Motorola Response

Comply.

Our service architecture natively aligns with NENA i3 standards (including NENA-STA-010.3f-2021). We enable long-term stability and security through stringent operational policies, rigorous certificate chain-of-trust handling, and a highly resilient, multi-cloud infrastructure.

Operational Policies & i3 Alignment

- **Modular Standards Compliance:** Our architecture is inherently modular, designed to seamlessly adapt to future NENA i3 revisions without requiring disruptive system overhauls or abandoning existing functionality.
- **Policy-Based Routing (PRF):** Routing logic is completely decoupled from technological constraints. Authorized administrators utilize a PRF to establish customized rules tailored to specific operational workflows and dynamic alternate routing needs.

- **Strict ITIL Change Management:** All operational modifications are governed by a formal ITIL-based framework. A Change Advisory Board (CAB) mandates rigorous impact assessments and executable rollback plans before any routing or network changes are promoted.

Certificate Chain-of-Trust Management

- **Managed PKI Issuance:** Motorola assumes full operational responsibility for provisioning and managing all certificates required for NGCS elements and PSAP interconnections.
 - **NIOC PCA Integration & Cross-Signing:** Until the NIOC PCA is fully deployed, we operate an RSA 2048-based ICA as a regional trust anchor. We explicitly commit to cross-signing this ICA with the National PCA (or utilizing NIOC-issued certificates directly) to ensure a seamless, long-term interoperability of trust chains.
 - **Continuous Automated Validation:** All SIP connections mandate mutual authentication via CA-signed certificates. Our systems enforce absolute trust through continuous, automated validation of CA signatures, distinguished names, active dates, and active querying of CRLs to instantly reject compromised credentials.
-

- Test/validation evidence showing interoperability and conformance with i3 JWS processing & verification across relevant services.

Motorola Response

Comply.

Aligning with our current implementation roadmap, we conduct rigorous internal and third-party testing to validate JWS processing, Base64 encoding, and cryptographic verification specifically for our compliant i3 Logging Services.

- **NENA ICE Interoperability Testing:** We actively participate in NENA Industry Collaboration Events (ICE). During these rigorous, vendor-neutral testing events, our Logging Service's ability to successfully ingest, verify, and store JWS-formatted LogEvents generated by third-party i3 functional elements is tested, validated, and documented for cross-vendor interoperability.
- **Internal QA & Automated Validation:** Our internal Quality Assurance (QA) protocols utilize automated CI/CD pipeline testing to validate strict NENA-STA-010.3 conformance before any software release. This includes automated test cases verifying proper JWS payload construction, header formatting, and accurate cryptographic signature verification.
- **Byte-for-Byte Evidentiary Auditing:** We conduct continuous validation testing to ensure the Logging Service stores the entire JWS exactly as received. These tests verify that the system retains the documents byte-for-byte unaltered, mathematically proving the cryptographic signature remains perfectly intact for legal chain-of-custody requirements.
- **Future Policy Store Validation:** As our Policy Store JWS functionality (currently on our engineering roadmap) enters active development, it will be subjected to this same framework of strict internal QA and independent NENA ICE interoperability validation before general availability.

In the interim, while JWS Policy Store functionality is in development, all routing rules and access policies are strictly protected against unauthorized alteration through our centralized RBAC and Zero Trust architectural boundaries.

4.6 Information Privacy

All NG911 protocol operations must be privacy-protected in transit with TLS, and confidential data must be encrypted at rest, in conformance with the NENA i3 Standard and NG-SEC (NENA-STA-010.3 §5.8 & NENA-STA-040.2 §6.22). Implementations must support AES-256 (or stronger equivalent). Algorithms and key lengths must be chosen to protect data for the full retention period. Encryption keys must never be stored in plaintext; with access following a documented management policy – including strong passwords and multifactor authentication required for access. Alternative algorithms are acceptable only if cryptographically equivalent to, or stronger than, AES-256 with end-to-end interoperability support. The contractor should prepare for the ability to upgrade or replace encryption algorithms and parameters to ensure continued conformance with future updates to the NENA i3 and NG-SEC Standards.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A statement of conformance to NENA i3 and NG-SEC privacy & encryption requirements (NENA-STA-010.3 §5.8 & NENA-STA-040.2 §6.22).

Motorola Response

Comply.

Motorola formally confirms that our service conforms to the privacy and encryption requirements set forth in NENA-STA-010.3 §5.8 (Privacy) and NENA-STA-040.2 §6.22 (Data Protection).

- An architecture/configuration overview showing TLS everywhere in transit and encryption at rest for stored confidential data, with cipher/algorithm policies and downgrade protections.

Motorola Response

Comply.

Our service employed end-to-end encryption to ensure no data is left exposed:

- **In Transit:** All protocol exchanges (SIP, HTTPS, MSRP) are protected by TLS 1.2/1.3 utilizing Mutual Authentication (mTLS).
- **At Rest:** Confidential data, including CDRs and Incident Data (EIDOs), is encrypted using AES-256 or equivalent FIPS-validated algorithms.

- **Downgrade Protections:** We disable legacy protocols (e.g., SSL v2/v3, TLS 1.0/1.1) and weak ciphers (e.g., DES, RC4). Interfaces are configured to reject any connection attempt that does not meet the mandatory security baseline.
-

- A cryptographic longevity rationale demonstrating algorithms and key lengths cover the full data lifecycle. A key management policy: generation, storage, access control, rotation, backup/restore, and revocation; identification of key custodians and audit practices.

Motorola Response

Comply.

Our cryptographic selections are based on **NIST SP 800-57** and **NIST SP 800-131A** guidelines for long-term data protection.

- **Algorithm Selection:** We utilize **AES-256** for symmetric encryption and **RSA-3072** or **ECC (P-384)** for asymmetric operations, which are rated to provide security beyond the year 2030.
 - **Lifecycle Alignment:** This ensures that even if data is archived for a longer time period, the encryption remains resistant to brute-force attacks during that period.
-

- A key management policy: generation, storage, access control, rotation, backup/restore, and revocation; identification of key custodians and audit practices.

Motorola Response

Comply.

We manage cryptographic keys through a formal, documented lifecycle:

- **Generation:** Keys are generated within FIPS 140-2/3 Level 3 HSMs.
 - **Access & Custodians:** Access is restricted to designated Key Custodians (Security Administrators) using MFA and "M-of-N" multi-party control.
 - **Rotation & Backup:** Keys are rotated annually or upon a "Mover" event. Backups are stored in an encrypted state in physically secure, off-site vaults
-

- Operations evidence proving only approved algorithms are enabled and weaker ones disabled; include exception handling and a migration plan for any legacy endpoints.

Motorola Response

Comply.

Operational Evidence: Our service security function performs continuous scanning to verify that only approved algorithms are active.

- **Exception Handling:** If a legacy endpoint (e.g., an older PSAP gateway) cannot support modern encryption, it is isolated in a DMZ and connected via a secure proxy.
 - **Migration Plan:** These exceptions are time-bounded; Motorola works with the agency to upgrade the hardware or software to achieve full SHA-256/AES-256 compliance.
-

- If proposing alternates, a strength & interoperability justification confirming parity with AES-256 and end-to-end support across all impacted components.

Motorola Response

Comply.

Motorola does not propose alternatives to the AES-256 and RSA/ECC standards. We confirm that our end-to-end architecture supports these encryption algorithms across all NGCS and ESInet components ensuring seamless interoperability and consistent security.

4.7 Security Assessment and Audit

A cybersecurity assessment/audit verifies conformance/compliance with security requirements, controls, and standards. At a minimum, assessments/audits shall apply the impact categories (low, moderate, high) and security objectives (confidentiality, integrity, availability) defined in NIST FIPS 199 when assessing findings, and use those categories and objectives – together with vulnerability and threat information – to determine risk and remediation priority.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- An audit methodology that applies NIST FIPS 199 impact categories and security objectives and explains how impact × likelihood (or equivalent) drives risk ratings and prioritization.

Motorola Response

Comply.

Impact Categorization: We apply **FIPS 199** standards to categorize every system component based on the "high-water mark" of three security objectives:

- **Confidentiality, Integrity, and Availability (CIA):** Given the life-safety mission of NG9-1-1, core components (e.g., ESRP, ECRF) are categorized as High Impact, where a loss of availability would have catastrophic effects on agency operations.

- **Risk Calculation:** Risk ratings are derived using the formula: Risk = Impact x Likelihood.
 - **Impact:** Determined by the FIPS 199 category (Low, Moderate, High).
 - **Likelihood:** Based on current threat intelligence and the presence/effectiveness of mitigating controls.
 - **Prioritization:** This methodology ensures that a "High Impact" system with a "High Likelihood" of vulnerability exploitation receives immediate remediation priority over lower-impact findings.
-

- The proposed audit scope and cadence – initial baseline and periodic re-evaluation – including coverage of ESInet segments, NGCS components, PSAP-facing interfaces, and policy/procedure controls.

Motorola Response

Comply.

Motorola proposes a tiered audit schedule to maintain a continuous security baseline:

- **Initial Baseline:** A full-stack Security Assessment Report (SAR) is completed prior to the "Go-Live" of any NG911 resource, verifying conformance with NENA i3 and NIST 800-53 controls.
 - **Periodic Re-evaluation:**
 - **Annual Comprehensive Audit:** Independent assessment of ESInet segments, NGCS components, and PSAP-facing interfaces.
 - **Quarterly Control Reviews:** Focused audits of policy/procedure controls, including access recertification and change management logs.
 - **Continuous Scanning:** Automated vulnerability scans across all IP-reachable infrastructure.
-

- A findings lifecycle including severity assignment using FIPS 199 impacts, remediation due dates, owner assignment, tracking to closure, and verification of issue remediation.

Motorola Response

Comply.

All audit findings are managed through a formal Plan of Action and Milestones (POA&M):

- **Severity Assignment:** Findings are assigned a severity (Critical to Low) based on the FIPS 199 impact of the affected system.
 - **Owner Assignment:** Each finding is assigned a dedicated Remediation Owner from the Motorola Security team.
 - **Remediation Due Dates:** Strictly enforced based on severity (e.g., Critical findings due within 30 days).
 - **Verification:** Once remediation is complete, an independent assessor performs re-testing to verify the issue is closed before the finding is officially removed from the POA&M.
-

- Integration points with the Risk Management program and with continuous monitoring for follow-up testing of high-severity items.

Motorola Response

Comply.

The audit program is not a siloed activity but is fully integrated into our operational security posture:

- **Risk Management Integration:** Audit findings are fed directly into the Project Risk Register, allowing the State to make informed "Authorization to Operate" (ATO) decisions.
 - **Continuous Monitoring:** High-severity items identified during audits, trigger enhanced alerts within our NSOC.
 - **Follow-up Testing:** Any high-severity remediation is subjected to out-of-band follow-up testing (e.g., targeted penetration testing) to ensure that the fix is resilient against the specific threat vector identified.
-

4.7.1 Assessment and Audit Documentation

Security requirements and risk considerations must be built into development and delivery. Before deployment, every NG911 resource must complete a documented security assessment verifying conformance/compliance with applicable policies and/or requirements. Related components may be assessed as a group when appropriate. Assessment records must be retained as auditable evidence for future reviews.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A pre-deployment security assessment process covering all components with acceptance criteria, approvers, and required evidence.

Motorola Response

Comply.

We conduct a standards-based pre-deployment assessment and hardening process before any system transitions to production. This ensures an uncompromising security posture and functional stability before your "Go Live" event.

- **Security Assessment & STIG Hardening:** We execute initial Risk Assessments based on NIST SP 800-30, paired with comprehensive vulnerability scanning upon system turn-up. To actively minimize the attack surface, systems are strictly hardened in compliance with NENA NG-SEC standards and applicable DISA STIGs, configuring devices with only the absolute minimum applications, permissions, and access rights necessary for operation.

- **Rigorous Acceptance Criteria (SATP/FATP):** Systems must pass phased validation, starting with a Staging Acceptance Test Plan (SATP) to verify factory configurations, and culminating in a Final Acceptance Test Plan (FATP) for functional and failover testing. Crucially, no system is accepted with unresolved Severity 1 or Severity 2 issues. Additionally, a pre-migration checklist mandates a proven, stable environment before any PSAP cutover.
 - **Comprehensive Evidentiary Artifacts:** We provide transparent, documented proof of system readiness, including:
 - Independent third-party validation of mandatory requirements and features.
 - Complete SATP/FATP test results, raw SIP messaging logs, i3 functional element logs, and CDRs.
 - Formal vulnerability reports and independent security audits verifying compliance.
 - Written certification confirming the system is fully installed, configured, and ready for testing.
 - **Collaborative Approval & Client Authority:** Any pre-deployment system changes are strictly governed by our Cybersecurity team and Change Advisory Board (CAB). Final system acceptance requires a joint, formal sign-off, ensuring your agency's critical stakeholders retain ultimate authority over the final "Go Live" decision.
-

- Templates and examples of deliverables (control test results, residual risk statements, exceptions & compensating controls, approval sign-off) mapped back to requirements.

Motorola Response

Comply.

To protect the integrity of our security methodologies and the confidentiality of our existing client environments, Motorola maintains these specific deliverable templates and example artifacts as internal proprietary documentation.

Detailed samples of control test results, residual risk statements, and mapped exceptions contain sensitive architectural insights and procedural Intellectual Property and are therefore maintained as internal-only documentation to ensure the continued security and integrity of our systems and client environments.

- A documentation retention & evidence management plan supporting internal and third-party audits/assessments.

Motorola Response

Comply.

Our evidence management framework ensures all assessment records are securely retained and readily available for internal reviews and third-party audits.

- **Centralized Evidence Repository:** All project documents, RFCs, and Quality Review and Approval Records (QRAR) artifacts are secured within a centralized repository utilizing strict versioning control.

- **Long-Term Retention Policies:** We maintain strict, configurable retention periods. Contractual and process records, system data and reports (including assessment approvals) are retained for mutually agreed upon terms.
 - **Third-Party Audit Readiness:** This documentation framework directly supports rigorous independent scrutiny, enabling our continuous ISO 9001:2015 and ISO 27001 certifications, as well as our comprehensive SOC 2 Type 2 attestations.
-

- Integration points with change management and release processes to ensure no promotion to production without a complete, approved assessment.

Motorola Response

Comply.

We integrate our risk management and software release processes through an ITIL-based Change Management framework. This guarantees that no system changes, updates, or security patches ever reach the production environment without comprehensive documentation, testing, and explicit stakeholder approval.

- **Mandatory Risk & CAB Oversight:** Every service change request requires a formal risk assessment. Our Cybersecurity team actively participates in the Change Advisory Board (CAB) to rigorously evaluate the security impact of any proposed release before authorization.
 - **Initiation & Impact Assessment:** Engineering staff thoroughly evaluate every proposed change to accurately map its potential operational impact, risk profile, timeline, and associated costs.
 - **Rigorous Planning & Testing:** Before any deployment, a comprehensive implementation plan is developed and tested in a sandbox environment. This includes a mandatory rollback (back-out) strategy to instantly revert changes if unforeseen anomalies occur.
 - **Formal Stakeholder Approval:** A service change request can be halted at any stage. A release is only scheduled for production deployment after explicit, final authorization is secured from all engaged parties, including your designated agency representatives.
 - **Post-Implementation Revalidation (PIR):** Following execution, the release undergoes a documented Post Implementation Review. If the change addressed a security vulnerability, we mandate an immediate rescan and revalidation of controls to conclusively verify successful remediation.
-

- A tracking mechanism linking assessment findings/exceptions to remediation or formal risk acceptance and verification of closure.

Motorola Response

Comply.

We utilize our enterprise ITSM platform, ServiceNow, to provide an unbroken chain of custody for all security findings, tracking them from initial identification directly through to remediation, formal risk adjustment, and verified closure.

- **Identification & Reporting (QRAR):** We conduct rigorous quarterly baseline control reviews. Any identified control exceptions trigger a technical risk reassessment, which serves as the primary input for the system's Quarterly Risk Assessment Reporting (QRAR).
 - **Automated Remediation Linkage:** QRAR findings are instantly converted into actionable ITSM workflows. Standard vulnerabilities spawn formal Change Requests, while severe risks immediately declare an Incident and trigger an Emergency Change Request for rapid mitigation.
 - **Formal Risk Acceptance:** If a finding dictates a permanent change of controls or formal risk acceptance, it is systematically documented, tracked, and accommodated through our strict Change Management process, ensuring no risk is ever quietly bypassed.
 - **Mandatory Verification of Closure:** We require definitive proof of remediation. A security finding is only marked "closed" after a mandatory post-change scan and revalidation explicitly verifies that the vulnerability was successfully neutralized.
 - **Project-Level Deployment Tracking:** During initial system implementation (before operational steady-state), all assessment findings are managed via targeted Action Logs and a Project Punch List. Defects remain actively open until corrective action is verified and mutually signed off by both the Motorola and Customer Project Managers.
-

4.8 Security Monitoring, Detection, and Alerting

4.8.1 Security Event Logging and Continuous Monitoring

Security event logging is essential for early detection, scoping, and investigation of cybersecurity incidents. Logging should be centralized and standardized, tuned to capture only what is necessary, and informed by a baseline of "normal" activity so anomalies can be detected. While "Security Event Logging" objects for the NG911 Logging Service are not yet defined, the contractor's proposed solution must be ready to adopt them when published and leverage current standardized log retrieval functions.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Time synchronization controls proving all logging applications and device clocks align to the time server requirements from NENA-STA-040.2 §5.6.1, enabling cross-system correlation.

Motorola Response

Comply.

Our proposed solution includes NENA-compliant time synchronization across all systems to guarantee flawless, end-to-end event correlation and forensic logging accuracy.

- **High-Availability NTP Infrastructure:** We deploy an enterprise-wide Network Time Protocol (NTP) solution to provide reliable and secure time synchronization source. This infrastructure is configured for high availability across geographically diverse facilities.
 - **Precision GPS Synchronization:** To maintain absolute accuracy across the network, all NTP elements are synchronized via GPS signals to within a few milliseconds. Every functional element, infrastructure component, and network device within the architecture actively synchronizes time to NTP infrastructure.
 - **Flawless Cross-System Correlation:** By anchoring every system component to a single, precision time source, we guarantee absolute timestamp consistency across all event records, reports, and logs. This exact time-stamping is a foundational business rule of our NENA-compliant i3 Event Logger, enabling investigators and administrators to accurately correlate call flows, SIP messaging, and network events from end to end without discrepancy.
-

- A centralized logging architecture (collection, transport, storage) with coverage to trace and correlate events end-to-end across ESInet/NGCS; include any additional logging for administrative accounts.

Motorola Response

Comply.

Our proposed solution includes a centralized, cloud-native logging architecture to deliver comprehensive, end-to-end reporting to include all NGCS, ESInet and call handling CDR data.

Centralized Collection & Defensible Storage

- **Near Real-Time i3 Event Logging:** Operates 24x7x365 as a transaction logger, aggregating raw SIP messaging, HELD queries, LoST queries, and network traffic data from all FEs.
- **Precision Synchronization:** Utilizes a GPS-synchronized, NENA-compliant NTP master clock to timestamp every event, ensuring exact cross-system correlation.
- **Tamper-Proof Chain of Custody:** Data is securely uploaded via an i3-compliant interface and stored to prevent tampering, guaranteeing legal defensibility in court.
- **Data Retention:** Retention periods are highly configurable.

End-to-End Traceability & Correlation

- **Unified Visibility:** Seamlessly integrates NGCS i3 event logs, PSAP CDRs, and Text-to-9-1-1 data into a single, unified reporting interface.
- **Complete Call Flow Analysis:** Administrators can trace a call down from ingress, through NGCS core routing (ESRP, ECRF, LVF), to the final PSAP disconnect.
- **NG9-1-1 Call Viewer:** Technical staff can query a specific Call Identifier to extract a consolidated, chronological trace of every network event and SIP message generated across all system components.

Comprehensive Security & Administrative Auditing

- **Security & Access Logs:** Captures granular logs of all network traffic, IDS/IPS security alerts, and both physical and logical access attempts (permitted and denied) down to the virtual device level.

- **ITSM Change Management:** All maintenance activities, configuration modifications, and administrative requests are tracked via ServiceNow, providing a transparent audit trail accessible via the CWP.
 - **Data Discrepancy Tracking:** Logs all administrative updates to the LDB and GIS SI Discrepancies (e.g., "No Record Found" errors) are tracked from initiation to resolution to ensure full operational accountability.
-

- A review/monitoring cadence: at minimum weekly human review, plus a plan to reach near real-time visibility via automation (e.g., SIEM).

Motorola Response

Comply.

Our proposed solution provides near real-time threat visibility through advanced automation, paired with human oversight and a rigorous, structured review cadence to continuously validate system health and security.

- **Automated Threat Detection (SIEM & ML):** We deploy advanced SIEM tools empowered by machine learning to continuously aggregate logs, correlate network traffic, and automatically detect anomalies indicative of cyber threats.
 - **Local Integration & Dashboards:** Authorized personnel maintain near real-time network visibility via the CWP.
 - **24x7x365 NSOC Monitoring:** Far exceeding standard weekly checks, our NSOC is staffed continuously by expert public safety security analysts. These analysts actively investigate SIEM and IDS/IPS alerts in real time to initiate immediate threat mitigation.
 - **Structured Operational Cadence:**
 - **Deployment Phase:** Weekly or bi-weekly risk, progress, and action-item reviews led by your dedicated Project Manager.
 - **Post-Live Operations:** Formal monthly and quarterly operational reviews evaluating SLA adherence, system health, and incident resolution.
 - **Security & Access Audits:** Monthly vulnerability assessments of all physical and logical ACLs and baseline security controls.
-

- Log integrity & access protections: controls preventing deletion/modification, role-based access, retention periods, and storage locations that satisfy retention requirements.

Motorola Response

Comply.

We engineer our logging architecture to ensure data integrity by enforcing tamper-proof storage, zero-trust access controls, and highly resilient retention policies, ensuring all records remain legally defensible.

- **Tamper-Proof Integrity & Chain of Custody:** Our i3 Event Logger functions as a highly secure "transaction logger." To preserve a strict chain of custody and legal admissibility in court, CDRs are immutably stored in their original XML format. All events are precisely timestamped utilizing a NENA-compliant, GPS-synchronized NTP service to ensure exact chronological sequencing.
 - **Strict RBAC & Multi-Tenant Partitioning:** System access is tightly governed by RBAC and the principle of least privilege. The platform supports secure multi-tenant partitioning, siloing log and call data visibility by specific user role, PSAP, or jurisdiction. Furthermore, MFA is strictly mandated for all external portal and dashboard access.
 - **Configurable Long-Term Retention:** Data retention schedules are highly customizable to align directly with your agency's policies and state laws.
 - **Resilient Storage:** Transactional logs are actively maintained across dual repositories in separate data centers and securely aggregated within a centralized, cloud-native database. We strictly enforce geographic boundaries: all non-public data, including backups and disaster recovery data, remains exclusively within the United States.
-

- Tuning & performance practices showing log scopes/levels calibrated for detection without degrading performance; include the method to establish and update behavioral baselines.

Motorola Response

Comply.

Our proposed solution includes continuous security monitoring, deep packet inspection, and event logging, which will never degrade the performance or availability of mission-critical 9-1-1 routing elements. We achieve this zero-impact security posture through architectural tuning and dynamic, baselining.

Zero-Impact Security Monitoring

- **Offloaded Analysis:** Log aggregation and intensive security analysis are actively offloaded to our centralized NSOC, completely removing processing overhead from live edge network nodes.
- **Optimized Database Replication:** Heavy reporting and data replication tasks run exclusively on master databases. This intentionally isolates the processing load, preserving child database capacity entirely for live routing and location (LoST) queries.
- **Targeted Deep Packet Inspection (DPI):** IDS/IPS deep-level packet inspection is strictly isolated to the edge points interfacing with untrusted networks, ensuring internal core processing remains untouched by intensive traffic scrutiny.
- **Rate-Limited Scanning:** To eliminate the risk of traffic saturation, live penetration testing on production systems is prohibited. We rely instead on predictive monitoring and vulnerability scanning configured with strict rate-limiting.

Dynamic Baselines

- **Historical Normative Tracking:** The NSOC continuously aggregates metrics to establish historical performance trends, instantly triggering alerts upon any significant deviation from established normative values.

- **Quarterly Baseline Validation:** Administratively, all security controls and behavioral baselines undergo a mandatory, rigorous quarterly "true-up." This technical reassessment evaluates risk, identifies exceptions, and formally updates the accepted security baseline of the deployment.
-

- Forward-compatibility commitment to adopt forthcoming NG911 Security Event Logging specifications on release, including mapping/schema updates for integration with the NG911 Logging Service.

Motorola Response

Comply.

Our proposed solution provides compliance and seamless adaptation to evolving NENA i3 standards, ensuring your NG9-1-1 security, logging, and schema mappings remain at the forefront of industry best practices.

Forward-Compatibility & Architectural Agility

- **Guaranteed Adoption Timelines:** We commit to incorporating newly ratified IP network, security, and schema standards into our solution within 18 months of official industry ratification.
 - **Modular Microservices Architecture:** Our scalable design allows for incremental, non-disruptive software updates. This ensures your system effortlessly adapts to future NENA i3 revisions without requiring complete system overhauls or abandoning existing functionality.
 - **Proactive Roadmap Integration:** As standards evolve, our engineering teams actively review proposed updates, automatically incorporating them into our product development roadmaps to guide the continuous evolution of your service.
-

4.8.1.1 Time Synchronization

Accurate, consistent time underpins authentication, logging/correlation, troubleshooting, and continuous monitoring across the ESInet & NGCS. All elements must implement NTP (RFC 5905) and synchronize to a common, resilient time source consistent with NENA-STA-010.3 ('Time' §2.2 & 'Time Server' §4.17). The ESInet must provide an authoritative NTP service backed by a hardware clock or synchronized to external sources with sufficient redundancy to maintain local time during isolation. Service accuracy must be $\pm 1\text{ms}$ from true time, and the absolute time difference between any two elements within the ESInet/NGCS must be ≤ 0.1 second.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Time architecture showing the ESInet NTP service, upstream sources/hardware clocks, and redundancy/backup design.

Motorola Response

Comply.

Our proposed ESInet time architecture is designed for high availability and sub-millisecond precision, utilizing a multi-tiered hierarchy that anchors all network elements to redundant, hardware-backed atomic references.

1. Upstream Sources & Hardware Clocks

The architecture begins with **Stratum 0** high-precision hardware.

- **Primary Reference:** Each infrastructure region utilizes a fleet of redundant, satellite-connected **Atomic Reference Clocks** (GPS/GNSS) and Cesium oscillators.
- **Hardware Interface:** For mission-critical ESInet elements, we utilize a **Precision Hardware Clock (PHC)** interface. This allows the OS to bypass the standard network stack, communicating directly with the underlying physical hardware clock to eliminate micro-oscillations and network jitter.

2. ESInet NTP Service Layer

The middle-tier provides a distributed, highly available synchronization service for all IP-based emergency components.

- **Internal Endpoint:** A dedicated, anycast-addressed NTP service is exposed within the private network (e.g., via a link-local IPv4/IPv6 endpoint). This ensures that every element—from call-handling agents to database nodes—references the same regional clock source.
- **Protocol Support:** The service supports **NTPv4** for broad compatibility and **PTP (Precision Time Protocol)** for elements requiring microsecond-level accuracy.

3. Redundancy & Backup Design

To ensure "never-down" timing, the architecture employs a three-layer redundancy model:

- **Geographic Redundancy:** Each ESInet node is configured to poll multiple independent time-sync endpoints across different availability zones. If the local regional source becomes unreachable, the system automatically fails over to a neighboring region's reference clock.
- **Source Diversity:** In the event of a GPS signal loss or satellite interference, the infrastructure reverts to secondary onboard **Rubidium holdover oscillators**. These provide stable, high-accuracy timing for an extended period until the primary signal is restored.
- **Local Daemon Resilience:** All network elements run an intelligent time-sync daemon (such as *chrony*). These daemons are configured to ignore "falseticker" sources and use sophisticated filtering algorithms to maintain a stable local clock even if upstream network conditions degrade.

-
- Element compliance evidence that all ESInet/NGCS elements support NTP (RFC 5905) and are configured to the designated time sources.

Motorola Response

Comply.

We confirm full compliance with the requirement that all ESInet and NGCS FEs support NTP in accordance with RFC 5905 and are configured to synchronize with designated, authoritative time sources. Our solution ensures consistent, accurate time synchronization across all ESInet and NGCS components, supporting reliable event correlation, logging, security functions, and operational integrity throughout the i3 environment.

- Accuracy & drift SLAs proving $\pm 1\text{ms}$ at the ESInet time service, and 0.1 second max element-to-element skew; include monitoring and alerting for out-of-tolerance conditions.

Motorola Response

Comply.

Our cloud-native architecture leverages high-precision, hardware-backed time synchronization to meet and exceed the $\pm 1\text{ms}$ accuracy and 0.1s element-to-element skew requirements.

1. Accuracy & Drift Proof ($\pm 1\text{ms}$)

The solution utilizes a Precision Time Protocol (PTP) or Stratum-1 equivalent architecture. Instead of relying on variable internet-based NTP, our environment synchronizes directly with a local, satellite-connected atomic reference clock located within the regional infrastructure.

- **Mechanism:** By using a local hardware-clock interface (e.g., PHC), we eliminate network jitter and "asymmetric path" delays typical of standard NTP.
- **Result:** This ensures a steady-state accuracy of **<1ms** relative to UTC, providing the high-fidelity timestamps required for ESInet logging and call-event sequencing.

2. Element-to-Element Skew (0.1s Max)

To maintain a maximum 0.1s skew between all network elements, the system employs high-frequency polling and low-latency local synchronization.

- **Uniformity:** All instances, databases, and microservices within the environment sync against the same synchronized regional clock source, ensuring horizontal consistency.
- **Drift Correction:** Client-side daemons (such as **chrony** or high-accuracy **w32time**) are configured with aggressive "MinPoll" intervals to correct minor oscillations before they can accumulate into measurable skew.

3. Monitoring & Alerting for Out-of-Tolerance Conditions

Continuous verification is managed through integrated telemetry that tracks the health of the time-sync subsystem.

- **Metric Collection:** We monitor the **Root Dispersion** and **System Offset** (the delta between the local clock and the reference source) in real-time.

- **Threshold Alerting:** Automated alarms are configured to trigger if the offset exceeds **0.5ms** (providing a 50% safety buffer before the 1ms limit is reached).
 - **Incident Response:** Alerts are dispatched via a centralized Management System (NMS), notifying operations teams immediately of any "Out-of-Tolerance" conditions to ensure rapid remediation and audit-trail integrity.
-

- Isolation resilience procedures to maintain accurate local time if upstream is unreachable.

Motorola Response

Comply.

Our architecture is designed to maintain high-accuracy time synchronization even in the event of a total loss of connectivity to upstream Stratum 0/1 sources or broader network isolation.

1. Local Hardware Holdover (Stratum 0/1 Isolation)

In the event that the primary satellite-linked atomic reference clocks become unreachable, the underlying physical infrastructure enters **Holdover Mode**.

- **Mechanism:** The host hardware utilizes high-stability **oscillators** (such as Rubidium or high-end OCXOs) that maintain precise timing without an external signal.
- **Performance:** These local oscillators are designed to keep the environment within high-tolerance drift limits for extended periods, ensuring that the ESInet remains synchronized internally even if "cut off" from the global GPS/GNSS network.

2. Hypervisor-to-Guest Synchronization

For virtualized elements, resilience is maintained through a direct hardware-clock passthrough that does not depend on traditional network routing.

- **VMCTimeSync / PHC:** Each virtual machine (VM) accesses the physical host's hardware clock via a dedicated integration service or a **Precision Hardware Clock (PHC)** device.
- **Isolation Benefit:** Because this synchronization happens at the hypervisor level, the VM maintains accurate time even if all external networking (VPC/VNet egress) is disabled or fails.

3. Intelligent Client-Side "Chrony" Management

We utilize advanced time-sensing daemons (e.g., **chrony**) on all OS instances to manage isolation intelligently.

- **Drift Learning:** The system continuously calculates the "drift rate" of the local software clock during normal operation.
- **Autonomous Correction:** If all upstream NTP/PTP sources become unreachable, the daemon switches to **orphan mode** or uses its recorded drift history to "steer" the local clock, preventing the rapid time-sliding common in standard NTP implementations.

4. Intra-Cluster Consensus

In a multi-node ESInet deployment, elements can be configured to use each other as secondary "peer" sources.

- **Peer-to-Peer Sync:** If a cluster loses access to the regional clock but maintains internal connectivity, the nodes will synchronize with one another. This ensures that even if absolute UTC accuracy drifts slightly, the element-to-element skew remains below the 0.1s requirement for consistent log correlation.
-

- Operational controls: change management for time sources, certificate/time coupling checks, log/time baseline verification, and periodic audits of time-sync configuration and performance.

Motorola Response

Comply.

We provide continuous integrity and accuracy of our time synchronization infrastructure through rigorous ITIL-based governance, automated cryptographic coupling, and continuous proactive auditing.

- **ITIL-Based Change Management:** All modifications, upgrades, or maintenance to master clocks and time servers are strictly governed by an ITIL-based framework. This mandates a formal service change request, a comprehensive risk assessment, an executable rollback plan, and a formal Post Implementation Review (PIR).
 - **Automated Cryptographic Coupling:** Accurate time synchronization is intrinsically tied to our Public Key Infrastructure (PKI). Automated validity testing explicitly verifies time coupling, guaranteeing that expired or prematurely deployed certificates are instantly rejected if used outside their precise validity period.
 - **Continuous Baseline Verification:** All i3 event logs utilize NENA-compliant hardware timestamps to ensure legal defensibility. Our Network Security Operations Center (NSOC) continuously analyzes these logs against established performance averages to detect anomalies, backed by a mandatory quarterly "true-up" of all baseline security controls.
 - **Routine Maintenance & 3rd-Party Audits:** Time synchronization is a formally mandated requirement within our overarching cybersecurity policy. Master clocks undergo scheduled routine maintenance and the entire time service architecture is subjected to proactive vulnerability scans (annually and post-major change) as well as independent, third-party security audits.
-

4.8.2 Denial of Service and Telephony Denial of Service (DoS/TDoS)

A DoS/TDoS attack attempts to render resources unavailable by overwhelming capacity or impeding traffic flow. ESInet providers must have plans and procedures to mitigate and manage DoS/TDoS events. An ESInet must be able to withstand the largest feasible Distributed Denial of Service (DDoS) or TDoS attack, which, as of the current version of NENA-STA-010.3, means ≥ 1 Tbps (terabit per second) of mitigation capacity. This can be achieved via a combination of network/BCF bandwidth and mitigation services.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A DDoS/TDoS resilience architecture demonstrating $\approx \geq 1$ Tbps (terabit per second) effective mitigation capacity across ESInet ingress, BCF/SBC, upstream carriers, and contracted mitigation services (including how capacity is measured and assured).

Motorola Response

Comply.

To address the requirement for a DDoS/TDoS resilience architecture with >1 Tbps effective mitigation capacity, our solution leverages the native, massive-scale infrastructure DDoS Network Protection, integrated with specialized SBC and Upstream Carrier scrubbing. Our architecture follows a "Defense-in-Depth" strategy, distributing the 1 Tbps+ mitigation burden across four distinct layers to prevent any single point of saturation.

Edge Layer

By utilizing hyperscale cloud providers, we tap into global anycast networks designed to absorb multi-terabit volumetric attacks before they reach the Virtual Private Cloud (VPC) or Virtual Network (VNet).

- **DDoS Network Protection:** Provides always-on monitoring and automatic inline mitigation at the edge. We have mitigated attacks exceeding 2.3 Tbps, well above the requirement. Leverages the global scale of the network to defend against the largest known network-layer attacks.
- **Global Accelerator / Front Door:** Traffic is ingested at the nearest Point of Presence (PoP), dispersing the attack volume geographically.

TDoS & Signaling Layer (ESInet Ingress)

TDoS requires specialized handling of SIP/RTP traffic that standard volumetric filters might miss.

- **SBC & BCF Hardening:** We deploy high-capacity SBC and BCF with rate-limiting policies specifically for INVITE floods and SIP signaling anomalies.
- **Adaptive Thresholds:** Utilizing Adaptive Tuning and Health Checks, the architecture adjusts thresholds based on real-time traffic baselines rather than static limits.

Upstream Carrier & Contracted Services

For traffic originating outside the cloud ecosystem, we maintain peering with Tier-1 Carriers and specialized scrubbing providers.

- **BGP Anycast & Flowspec:** We utilize BGP Flowspec to push mitigation rules to the carrier edge, dropping malicious packets before they even transit to our cloud ingress points.
- **Scrubbing Centers:** Contracted "Always-On" or "On-Demand" scrubbing centers provide an additional 2–5 Tbps of dedicated capacity to filter non-TCP/UDP specialized traffic.

To ensure the architecture meets the <1 Tbps requirement, we employ rigorous measurement and validation protocols.

Mitigation capacity is measured across three primary vectors:

- **Ingress Throughput (bps/pps):** Real-time monitoring of raw bits-per-second and packets-per-second at the edge.
- **Scrubbing Efficiency:** We track the "Drop-to-Pass" ratio. Effective capacity is defined as the maximum volume of malicious traffic the system can drop while maintaining <1% latency increase for legitimate traffic.
- **SBC Session Capacity:** Measured in CPS (Calls Per Second) and concurrent sessions to ensure the BCF does not experience memory exhaustion during a TDoS event.

Capacity Assurance.

We maintain SLAs with 3rd-party providers that guarantee "unlimited" or "best-effort" mitigation that historically exceeds 1 Tbps. Periodic DDoS simulations to stress-test thresholds and response playbooks. Motorola has direct access to the DDoS Response Team for 24/7 expert intervention during sustained high-volume events.

-
- Traffic re-route capability design showing how private links and any Internet-based paths can be redirected to a mitigation service during events; include activation triggers, propagation steps, and rollback.

Motorola Response

Comply.

Traffic re-route capability is included in our system design:

- **Activation Triggers:** Mitigation service is triggered automatically when traffic exceeds a pre-defined Signaling / Bandwidth Threshold (e.g., a 300% surge in SIP INVITES or 80% saturation of an ingress link).
- **Propagation & Reroute:** We utilize **BGP Flowspec** or **DNS redirection** to swing traffic from **private links and Internet-based** paths to the scrubbing centers. This occurs at the upstream carrier level, ensuring "dirty" traffic is discarded before it enters the States' network.
- **Rollback:** Once the Network & Security Operations Center (**NSOC**) confirms the attack has subsided (e.g., 30 minutes of "clean" baseline traffic), BGP routes are gracefully reverted to the original production paths.

-
- Plans and procedures to mitigate and manage DoS/TDoS incidents.

Motorola Response

Comply.

DDoS Specifics: Our playbooks include specific procedures for Telephony DoS (TDoS), such as:

- **White-listing:** Prioritizing traffic from known-good OSP gateways.

- **CAPTCHA for Callers:** Forcing non-emergency-originating traffic through an Interactive Voice Response (IVR) challenge to weed out automated "call-bots."
- **Black-holing:** Null-routing specific source IPs or geolocations identified as the attack origin.

DDOS playbook procedures are provided in the requirement above 'Traffic Rerouting capability'

- Operational testing evidence of re-route/mitigation cutovers and load exercises, with results demonstrating maintained call delivery and measured restoration times. Monitoring & detection of volumetric and signaling-layer abuse with alert thresholds and dashboards spanning network, BCF/SBC, and application layers.

Motorola Response

Comply.

Motorola provides evidence of resilience through annual load-testing exercises. We simulate scenarios where the system is subjected to higher signaling volumes than the average times for the State of Nebraska. Results demonstrate that our **ESRP** maintains call delivery integrity with restoration times (failover to mitigation) measured in seconds, not minutes.

- Monitoring & detection of volumetric and signaling-layer abuse with alert thresholds and dashboards spanning network, BCF/SBC, and application layers.

Motorola Response

Comply.

Dashboards: Our dashboard provides a unified view of the threat landscape.

- **Monitoring & Detection:** We monitor for **Signaling-Layer Abuse**, such as SIP "**Registration Storms**" or "**INVITE floods**," which aim to exhaust ESRP processing power rather than bandwidth.
 - **Thresholds:** Adaptive thresholds are set at the network edge to detect anomalies in real-time, providing dispatchers and administrators with a "**System Health**" status that reflects both network and application-layer stability.
-

- Configuration governance for temporary blocks/rate limits and rule updates during incidents, including audit trails and post-incident reviews.

Motorola Response

Comply.

The NSOC is authorized to implement **Temporary Rate Limits or blocks** during an active incident.

- **Audit Trail:** Every rule change is logged with a timestamp, the ID of the authorizing administrator, and the rationale for the change.

- **Post-Incident Review:** Every major DoS/TDoS event triggers a mandatory After-Action Report (AAR) to refine thresholds and ensure that temporary blocks are removed once the threat is neutralized.
-

4.8.3 Intrusion Detection and Prevention Systems (IDS/IPS)

The contractor must include intrusion detection to identify known threats and suspicious behavior across endpoints and networks, with alerts routed to a central monitoring function. Intrusion prevention adds automated blocking and must be carefully deployed to avoid disrupting 911 call handling; on segments carrying live call media and signaling, IPS should be avoided unless rigorously engineered, tested, and monitored. Controls must be tuned and maintained so detections remain accurate as the environment changes.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- **Architecture and placement:** where IDS is deployed, where IPS (if any) is deployed, and how alerts flow to a central SIEM; include rationale for deployed controls – ensuring no impact to legitimate media/signaling.

Motorola Response

Comply.

Motorola utilizes a layered IDS/IPS architecture to provide full visibility into the call path:

- **Placement:** Intrusion Detection System (IDS) sensors are deployed at the ESInet Ingress (OSP side) and within the **Management Zone** to monitor traffic without introducing latency into the call path. Intrusion Prevention system (IPS) is strategically active on the **BCF** and internal **firewalls** to block verified threats at the network edge.
 - **Alert Flow:** All telemetry (e.g., NetFlow, packet metadata, and security events) is forwarded via secure TLS tunnels to our Centralized SIEM for real-time correlation.
 - **Rationale:** By deploying IDS at the core and IPS at the boundary, we ensure that malicious traffic is blocked early while legitimate multimedia media/signaling (SIP/RTP) traverses the core with zero inspection-related delay.
-
- **Content currency & tuning:** processes to update signature content at least weekly and to review/update anomaly profiles at least annually and upon material changes; including tuning and drift management.

Motorola Response

Comply.

We maintain a rigorous lifecycle for threat intelligence:

- **Signature Updates:** Our **NSOC** automates signature updates at least weekly (and immediately upon high-severity vulnerability disclosures).
 - **Anomaly Profiling:** Anomaly profiles and behavioral baselines are reviewed annually and after material changes to the ESInet (e.g., adding a new PSAP or OSP).
 - **Drift Management:** We utilize automated "Tuning" cycles to identify signature drift—where updates may cause new false positives—ensuring the system adapts to the evolving 9-1-1 traffic environment.
-

- **Monitoring cadence:** procedures for at least weekly human reviews, with staffing/tools that achieve daily or near real-time monitoring; escalation paths and on-call coverage.

Motorola Response

Comply.

The security of the State of Nebraska ESInet is managed by our Public Safety NSOC:

- **Real-Time Monitoring:** We utilize automated SIEM correlation to provide near real-time monitoring of all IPS/IDS events.
 - **Human Review:** Our security analysts perform at least weekly deep-dive human reviews of all "Medium" and "Low" severity alerts to identify persistent or subtle threats.
 - **Escalation & On-Call:** We provide 24/7/365 on-call coverage with defined escalation paths for **critical** security incidents, ensuring a rapid response to any detected intrusion.
-

- **Configuration governance:** annual configuration reviews, change controls, test/validation before enabling prevention actions, and rollback procedures.

Motorola Response

Comply.

We apply strict controls to the configuration of security sensors:

- **Annual Reviews:** All IDS/IPS rule-sets and configurations undergo an annual formal review to ensure they remain aligned with NENA i3 security requirements.
- **Change Control:** Changes to IPS blocking rules follow a formal Change Management (CM) process.
- **Pre-Enforcement Validation:** Before any new "Prevention" (blocking) rule is enabled in production, it is tested in our Staging Environment to verify it does not inadvertently block legitimate 9-1-1 traffic.

- **Rollback:** Every configuration change includes a documented rollback procedure to restore the last-known-good state in the event of an operational issue.
-

- **Quality management:** metrics and methods to track and reduce false positives/negatives, periodic effectiveness reviews, and sample investigation records.

Motorola Response

Comply.

To ensure the integrity of emergency services, we proactively manage detection quality:

- **Metrics:** We track False Positive Rates (**FPR**) and False Negative Rates (**FNR**) as KPIs.
 - **Effectiveness Reviews:** Periodic reviews compare IDS/IPS logs against actual threat data to identify gaps in coverage.
 - **Investigation Records:** We maintain Sample Investigation Records that document the end-to-end handling of an alert, providing an audit trail for forensic and compliance purposes.
-

- **Integration:** how IDS/IPS telemetry correlates with firewalls, endpoint security, event logs, and SIEM; storage/retention aligned to logging requirements and protected against tampering.

Motorola Response

Comply.

Our IDS/IPS telemetry is a core component of the "Common Operating Picture":

- **Correlation:** Telemetry is automatically correlated in the SIEM with firewall logs, endpoint security (EDR) data, and mTLS authentication events. This allows our analysts to see, for example, if a blocked IPS signature originated from a device that also failed an authentication check.
 - **Storage & Retention:** Logs are stored in a **tamper-evident** environment. Retention is aligned with the NENA-STA-040.2 requirements, ensuring that forensic data is available for the full required audit period.
-

4.9 Domain Name System (DNS)

DNS is mission-critical for NG911 service reachability and must be engineered and operated to resist tampering and disruption (e.g., spoofing, cache poisoning, DoS on resolvers). The contractor shall implement defense-in-depth protections (DNSSEC validation/signing, logging, cache-locking, response-rate limiting), and align DNS administration with privileged account, patching, and change-management controls/requirements outlined elsewhere in this RFP.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- DNSSEC is enabled on all deployed DNS servers, and clients are configured to request DNSSEC validation.

Motorola Response

Comply.

- **Server-Side:** Motorola confirms that **DNSSEC** is enabled on all authoritative and recursive DNS servers within the ESInet. All zones are cryptographically signed using a secure chain of trust anchored by the national PCA or the DNS root.
 - **Client-Side:** All internal ESInet and NGCS FEs (clients) are configured to request and verify **DNSSEC** validation on all lookups, ensuring that any tampered or forged DNS responses are rejected before they can impact call routing.
-

- DNS logging is enabled on all DNS servers with centralized collection and retention; describe log scopes and how performance impact is managed.

Motorola Response

Comply.

- **Centralized Logging:** Detailed DNS query and response logging is enabled on all servers, with real-time forwarding to our centralized SIEM.
 - **Log Scopes:** Logging includes query type, source IP, response code and DNSSEC validation status.
 - **Performance Management:** To manage performance impact, we utilize asynchronous log forwarding and high-speed local buffers. This ensures that the overhead of logging does not introduce latency into the critical DNS resolution path for emergency services.
-

- Cache locking is enabled and set to 100% of TTL on recursive servers.

Motorola Response

Comply.

Our recursive resolvers are configured with **Cache Locking** set to 100% of the Time-to-Live (TTL). This security feature prevents an attacker from overwriting (poisoning) a cached record before its expiration, maintaining the integrity of service reachability for the duration of the record's validity.

- Response rate/time limits are configured on name servers to mitigate DoS/TDoS effects.

Motorola Response

Comply.

- **DoS/TDoS Mitigation:** To mitigate the effects of DNS amplification and query-flood attacks, we implement Response Rate Limiting (RRL).
- **Configuration:** Name servers are tuned to limit identical responses to specific subnets and to "slip" (truncate) responses during high-volume events, forcing legitimate clients to retry over TCP while dropping malicious volumetric UDP traffic.

- Administrative access controls to DNS infrastructure conform to requirements in NENA-STA-040.2 §6.2.1.3 'Administrator Accounts'.

Motorola Response

Comply.

- **Privileged Accounts:** In accordance with NENA-STA-040.2 §6.2.1.3, access to DNS infrastructure is restricted to authorized administrators using individual, non-generic accounts.
- **MFA & RBAC:** All DNS administrative actions require MFA and are governed by a RBAC model that enforces the principle of least privilege.

- Patch and update compliance for all DNS components conforming to requirements in NENA-STA-040.2 §5.5 'Patching and Updating' including emergency update procedures for critical CVEs.

Motorola Response

Comply.

- **Routine Patching:** DNS components follow the mandatory monthly patching cadence outlined in NENA-STA-040.2 §5.5.
- **Emergency Procedures:** For critical CVEs, we implement an Emergency Update Procedure designed to validate and deploy patches across the ESInet within 48 hours of availability, following an expedited change path.

- Network placement & resilience: DNS architecture diagrams showing internal vs. external roles, inter-site redundancy, diverse upstream resolvers, and protections at network boundaries.

Motorola Response

Comply.

DNS Architecture & Resilience

The Motorola ESInet DNS architecture is a multi-cloud, multi-region solution designed for high availability, inter-site redundancy, and strict functional separation between internal and external assets.

1. Network Placement and Functional Roles

The architecture employs a tiered strategy to isolate public resolution from private network traffic:

- **External/Public Roles:** Dedicated public DNS zones are hosted to resolve internet-facing services.
- **Internal/Private Roles:** Private hosted zones are deployed across all production environments to resolve services exclusively within the ESInet.
- **Boundary Protections:** Controlled inbound and outbound endpoints serve as secure gateways. Inbound endpoints manage Partner DNS requests, while outbound endpoints forward non-internal domain requests to designated Partner resolvers.

2. Inter-site Redundancy and Synchronization

To eliminate single points of failure, the design integrates:

- **Multi-Cloud Distribution:** DNS resolvers and private zones are replicated across our service
- **Automated Synchronization:** A dedicated pipeline maintains consistent DNS definitions across all providers and regions, preventing stale records during regional failovers.
- **Global Resolution:** Partners receive multiple DNS server endpoints across different cloud providers to ensure continuous resolution during a provider-specific outage.

3. Diverse Upstream Resolvers and Forwarding

The system adapts to various Partner hosting models:

- **Partner-Hosted DNS:** For partners maintaining independent DNS, the ESInet uses NS records to redirect name resolution to the partner's servers via outbound endpoints.
- **Motorola-Hosted DNS:** For partners utilizing Motorola's infrastructure, requests are resolved directly by the resilient DNS core

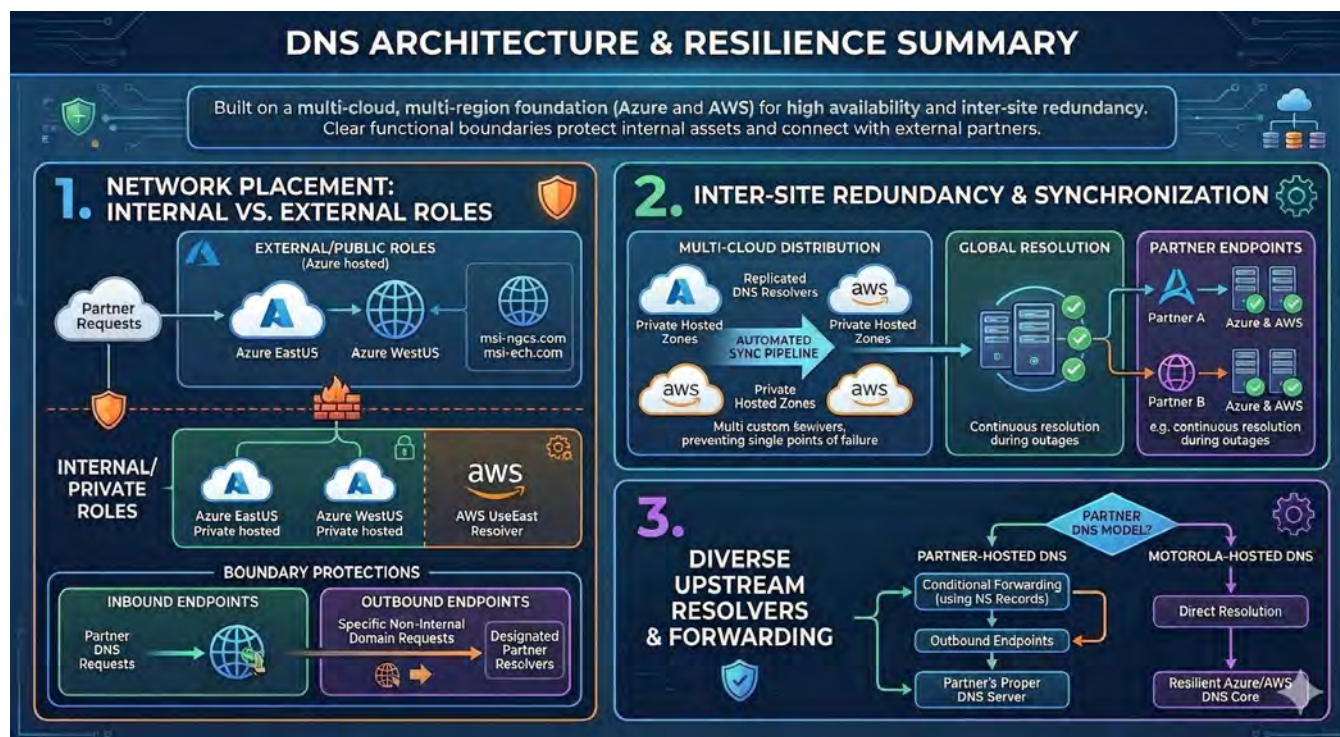


Figure 5-1: High Level DNS Architecture Diagram

- Monitoring and alerting for DNS health and integrity (e.g., DNSSEC validation failures, abnormal NXDOMAIN spikes, RRL hits).

Motorola Response

Comply.

Our NSOC provides 24/7/365 monitoring for DNS health and integrity:

- Validation Failures:** Automated alerts for any spike in **DNSSEC** validation failures, which may indicate an active spoofing attempt.
- NXDOMAIN Spikes:** Monitoring for abnormal spikes in **NXDOMAIN** responses, often a hallmark of a dictionary attack or TDoS event.
- RRL Hits:** Dashboards track real-time RRL mitigation events, providing immediate visibility into localized or wide-scale DoS activity targeting the 911 infrastructure.

5. Reporting Services Requirements

The contractor shall implement end-to-end logging for all call and transaction events across ESInet and NGCS components in RAW format. Logs must include ISO 8601 timestamps with time zone offset, unique correlation IDs, call identifiers, SIP message summaries (headers and SDP), PIDF-LO snapshots (privacy-redacted), routing decisions, ECRF/LVF responses, PSAP handoff timestamps, and error details. Logs shall be tamper-evident through cryptographic hashing or blockchain-like mechanisms and protected against unauthorized access.

Motorola Response

Comply.

The system shall generate CDRs for every emergency call, capturing fields such as calling line identifier, location used for routing, receiving PSAP ID, call start/answer/end timestamps, media types negotiated, disposition codes, and any transfers. CDR format and fields must align with NENA specifications, supporting export in XML/JSON.

Motorola Response

Comply with Clarification.

The Motorola Eclipse Analytics reporting platform stores all CDR associated with every call. Each call contains at a minimum call type, line identifier, location, PSAP ID, Call Start, Answer and End Times, media type, disposition and transfer events. Export of the CDR is in PDF report format.

Logs and CDRs shall be retained for a minimum of 7 years (or per jurisdictional policy), with secure storage, searchable indexing (e.g., via Elasticsearch), and export in standard formats (CSV, JSON, PDF). Access must be role-based, with audit trails for queries.

Motorola Response

Comply.

The contractor shall provide data to the PSC data analytics platform to allow for pre-built reports on call volume, average answer time, transfer metrics, location validation failures, and outage incidents, along with ad-hoc querying tools.

Motorola Response

Comply.

The system must maintain auditable trails for all configuration changes, GIS updates, and policy modifications, recording user identity, timestamps, before/after values, and rationale.

Motorola Response

Comply.

5.1 Reporting and Data Collection Requirements

The State requires enterprise-wide reporting and data collection capabilities on all aspects of the proposed NG911 system.

Motorola Response

Comply.

This capability must be agnostic to provider, system or technology and must be able to collect reportable data on the operation, configuration, and maintenance of the NG911 system. This includes both the NG911 systemwide/statewide/enterprise wide and local/PSAP specific data collection, logging and reporting necessary for the processing and documentation of 911.

Motorola Response

Comply.

5.2 Logging Service

The State requires that there be a Logging Service conforming to NENA-STA-010.3. The logging service must be capable of logging all **LogEvents** defined in NENA-STA-010.3, including media, and all FEs provided under the contract must generate such **LogEvents** and send them to the logging service.

Motorola Response

Comply.

The State desires that the Logging Service be made available to any PSAP that chooses to use it and implements the required i3 logging interfaces.

The Logging Service must support the query, retrieval, and log event replicator mechanisms described in NENA-STA-010.3.

Motorola Response

Comply.

The Logging Service must support `ElementState` and `ServiceState` SUBSCRIBE/NOTIFY per NENA-STA-010. The State must be able to subscribe to `ServiceState` and receive the standard state changes.

Motorola Response

Comply.

The proposal shall describe the Logging Service in detail.

Motorola Response

Comply.

Our Logging Service is a purpose-built NG9-1-1 event recording system designed for seamless integration within a NENA i3-compliant Next Generation Core Services environment. Operating as a native functional element on the ESInet, the Logging Service collects and preserves system events from across the Service, maintaining a complete, time-synchronized, and tamper-evident record of every transaction. A robust reporting engine surfaces event data through configurable dashboards and scheduled exports, giving agency administrators and PSAP managers actionable visibility into system activity, call handling trends, and operational metrics across the ESInet.

5.3 i3 Logging and Reporting Requirements

The proposed solution's NG911 logging and reporting system must conform to NENA-SAT-010.3 i3 logging requirements, including functional element logging, data collection, and reporting.

Motorola Response

Comply.

5.4 Functional Element Reporting

All functional elements within the ESInet (e.g., ESRP, ECRF, LVF, LIS, BCF) MUST be capable of reporting their operational status, critical events, alarms, and other relevant data. This reporting is essential for system monitoring, troubleshooting, security analysis, and performance management. Reporting mechanisms shall conform to standard protocols to ensure interoperability with a centralized logging and monitoring infrastructure.

- ESInet to PSAP Call Delivery transactions
- SIP Conference metrics
- PSAP Routing Duration Report
- Concurrent Calls
- BCF Session Reporting
- ESRP Session Reporting
- ESRP Queue State
- ECRF Session Reporting
- LVF Reporting
- LNG Session Reporting

Respondents must describe the proposed enterprise-wide NG911 logging, data collection, and reporting system and the elements provided above.

Motorola Response

Comply.

Our Logging Service collects and preserves operational status, critical events, alarms, and system events from all ESInet FEs, maintaining a complete, time-synchronized, and tamper-evident record across the Service infrastructure.

A robust reporting engine surfaces this data through configurable dashboards and scheduled exports covering the full scope of required reporting domains: ESInet to PSAP call delivery, SIP conference metrics, PSAP routing duration, concurrent call volumes, BCF and ESRP session activity, ESRP queue state, ECRF and LVF session reporting, and LNG session data. Agency administrators and PSAP managers gain actionable, enterprise-wide visibility into system activity, call handling trends, and operational metrics, fully conforming to standard protocols for interoperability with centralized logging and monitoring infrastructure.

All endpoints described send log events to redundant logging endpoints thereby enabling all of the metrics, visibility, and reporting functionality desired.

Standard Protocols and Interoperability

To ensure interoperability with a centralized logging and monitoring infrastructure, the logging service is optimized as a “transaction logger” and conforms to NENA-STA-010.3f-2021. Furthermore, the service provides an i3-compliant web services interface for the retrieval and reporting of all i3 event log data.

Required Reporting Elements

Our enterprise-wide reporting system natively tracks and reports on all operational statuses, critical events, and alarms for the FEs required by the State:

- **ESInet to PSAP Call Delivery transactions:** Identifies the number of incoming ESInet calls that are “serviceable,” and what percentage of those serviceable calls are delivered successfully to a PSAP across a given date range.
- **SIP Conference metrics:** Addressed via the PSAP Conference Summary report.

- **PSAP Routing Duration Report:** Provides high-level call delivery summary statistics for all calls delivered to the selected PSAP(s) by the ESInet.
 - **Concurrent Calls:** Generates a report showing the number of active, simultaneous calls traversing the network at any user-selected given time.
 - **BCF Session Reporting:** Contains a log, per user-selectable BCF, of all calls handled within a given date range. This report provides basic, high-level call details, and BCF processing time calculations for each processed call.
 - **ESRP Session Reporting:** Provides a log of all 9-1-1 sessions received and processed by the Emergency Services Routing Proxy (ESRP) selected by a user over a specified date range.
 - **ESRP Queue State:** Provides detailed information related to ESRP queue states when and where they are engaged or utilized within a user-selected date/time range.
 - **ECRF Session Reporting:** Provides a log of all 9-1-1 sessions received and processed by each user-selected ECRF over a selected date range.
 - **LVF Reporting:** Addressed via Location Validation Logging, which provides a log of location validations that occur over a selected date range.
 - **LNG Session Reporting:** Provides a log of all SIP INVITES generated by a user-selected LNG over a selected date range.
-

5.5 Monitoring, Outages, Failover, Trouble Tickets, and Escalation

The State requires that there be a Network Operation Center (NOC) that monitors the ESInet, the NGCS, the gateways, and all the other elements provided under the Contract. Each element must be continuously monitored for correct operation, and any faults must cause alerts to the NOC.

Motorola Response

Comply.

Any element failure must be treated as an outage. Any service failure must be treated as a serious outage. The proposal must include a description of outage classifications with escalation processes and notification processes. A system outage must have an escalation process that escalates to the highest non-executive level within the committed SLA. For example, an outage on a service with a 5-nines (99.999% uptime) SLA must escalate to the highest non-executive level within five (5) minutes of the outage. In this context, non-executive means all the contractor and appropriate subcontractor technical staff is committed at the highest level, but not necessarily senior executives who could monitor, but not actually contribute to problem resolution. A single person must be designated the owner of such an outage, and that owner must be empowered to direct any available resources to assess, diagnose and repair the cause or effect of the outage. The owner of the outage must be reported to the State promptly.

Motorola Response

Comply.

Our service and support models comply with the requirements to treat element and service failures as outages, utilizing a structured incident management system for classifications, escalations, notifications, and ownership.

Severity Level Classifications: We classify incidents into four severity levels. Any element or component failure is treated as an outage (Medium or High, depending on redundancy loss), and any full-service failure is treated as a serious/critical outage:

- **Critical (Priority 1):** Significant and/or severe degradation of service functionality that impacts inbound call or associated location processing, with no workaround available.
- **High (Priority 2):** Significant degradation of service functionality that impacts inbound call or associated location processing where a workaround may be available.
- **Medium (Priority 3):** A minor degradation of service functionality or capacity of inbound call or associated location processing.
- **Low (Priority 4):** A degradation of system functionality that does not impact inbound call or associated location processing.

Escalation Processes (within committed SLAs): We utilize automated SLA timers and escalation procedures to ensure the highest non-executive technical staff is fully engaged within the committed timeframes. Escalations are triggered based on the percentage of the SLA target response time that has elapsed:

- 50% of SLA elapsed: Escalated to the Assigned Engineer.
- 75% of SLA elapsed: Escalated to the Manager of the Assigned Engineer.
- 100% of SLA elapsed: Escalated to the Sr. Manager of Technical Service Delivery (the highest non-executive level).

Notification Processes: The 24x7x365 Network Security Operations Center (NSOC) manages all incident ticket handling and notifications.

- For critical events (Priority 1) that impact the delivery of 9-1-1 traffic, initial notification is provided to designated State and PSAP personnel discovery via phone call, email, or SMS text message.
- This initial notification conveys all available information useful for mitigating the effects of the outage, along with a ticket reference number and follow-up contact information.
- Progress updates are supplied continuously; Priority 1 issues receive hourly updates, and Priority 2 issues receive updates. Notifications are driven by the IT Service Management (ITSM) toolset (ServiceNow), and authorized users can also view real-time status via the CWP.

Outage Ownership and Resource Allocation: To manage an outage, we designate an Incident Manager who acts as the single owner of the event. The primary objective during an incident is to mitigate impact, and the Incident Manager is fully empowered to call upon whatever resources are required to assess, diagnose, and restore system functionality on a 24x7x365 basis.

We ensure the owner and all material information are reported to the State promptly. No later than one hour after the initial contact for Critical and High incidents, we provide updates that include the best-

known cause, geographic scope, estimated time for repairs, and any other information or personnel contacts useful to the management of the outage.

Any outage visible to any PSAP must be reported to that PSAP and to the State. The proposal must include the available notification methods and timing of reports of outage, progress, and restoration.

Motorola Response

Comply.

We utilize our ITSM toolset (ServiceNow) to automatically generate notifications for outages and service-impacting events based on defined thresholds. Designated PSAP and State personnel are notified via phone calls, emails, and SMS text messages. These notifications can include direct links to the associated trouble ticket for quick access. Additionally, authorized users have near real-time visibility into network status, route exceptions, and active tickets through the centralized CWP.

Timing of Initial Outage Reports: The 24x7x365 Network Security Operations Center (NSOC) manages all incident tracking, alerting, and escalations.

- **Critical (Severity Level 1):** For events involving a full loss of critical functionality (such as an inability to deliver 9-1-1 traffic), initial notification is provided on discovering the outage.
- **High (Severity Level 2):** For significant degradation of service where a workaround may be available, initial notification is provided.
- The initial notification conveys all available information useful for mitigating the effects of the outage, along with a ticket reference number and follow-up contact information.

Timing of Progress Updates: During an active outage, the NSOC provides continuous status updates to stakeholders until the service is fully restored:

- **Critical (Level 1):** Progress updates are supplied hourly (or at the beginning of every hour during the outage).
 - **High (Level 2):** Progress updates are supplied.
 - Furthermore, Motorola communicates additional material information—such as the nature of the outage, its best-known cause, geographic scope, and estimated time for repairs—as it becomes available.
 - **Timing of Restoration and Reason for Outage (RFO) Reports:** Following the restoration of normal 9-1-1 services, Motorola tracks the resolution and provides structured Reason for Outage (RFO) reports detailing the event:
 - **Preliminary RFO Report:** Delivered to the State and affected PSAPs of the initial issue.
 - **Final Event Analysis Report (EAR) / Root-Cause Analysis:** An in-depth final report detailing the full timeline, the root cause of the outage, and the preventive actions taken to avoid similar future occurrences is provided.
-

Any outage which causes an SLA failure for the month in which the outage occurred must be investigated, the root cause(s) must be determined, and corrective actions must be undertaken. The State and affected PSAPs must receive a report with the root causes, corrective actions and

with committed dates. Follow-up reports noting progress against the committed dates must be provided quarterly. The State expressly reserves the right to question the root cause determination and, if it determines that the proposed corrective action plan is deficient, the contractor and the State will negotiate in good faith to amend the root cause and form a corrective action plan that is mutually agreeable.

Motorola Response

Comply.

The State requires that the contractor provide a help desk, which may be the NOC or a different group. The help desk must be staffed 24/7/365 by staff qualified to solve the most common issues encountered by PSAPs. The help desk must have a ticketing system that accepts tickets submitted by website or telephone call. The help desk must be the exclusive mechanism used to report problems by PSAPs or State staff. Every problem report must generate a ticket.

Motorola Response

Comply.

For problem reports received by telephone, the call must be answered by a qualified technician within 60 seconds 90% of the time. For website entered tickets, an initial automated email must be generated immediately, and a follow up email or telephone call must be sent within 5 minutes 99% of the time. The technician first encountering a new issue must be able to solve the problem by taking whatever actions are required to close the ticket themselves 50% of the time. This should be included in a monthly report to offer KPIs.

Motorola Response

Comply.

The help desk must take ownership of all reported problems. Sustained effort must be maintained until the problem is solved and the ticket is cleared.

Motorola Response

Comply.

The State requires that the contractor integrate or “bond” the ticketing systems of each supplier or subcontractor which may be engaged by a ticket, so that the help desk is able to have full visibility and follow up as necessary with such suppliers and subcontractors. The help desk must maintain ownership of issues even if suppliers or subcontractors must solve all or part of the reported problems. However, while the help desk must maintain ownership of the issue, it is incumbent upon the contractor to keep the State informed and fully aware of progress during the effort to restore services. The State prefers that the reporting entity be able to converse with the people

who can solve the problem, so if a contractor is solving the problem, the State desires the help desk to keep abreast, but not be in the middle of solving the problem.

Motorola Response

Comply.

When sustained outages (more than 15 minutes) occur, the contractor must investigate and initiate workarounds to bring the system back to at least partial operational state. Even if the actual problem source has been found, and repairs underway, workarounds must be devised to ameliorate the problem if the work arounds can be completed faster than the actual problem repair.

Motorola Response

Comply.

5.6 Maintenance and Configuration Reports

Respondents must provide maintenance and configuration reports once a maintenance issue has been completed or an issue requiring maintenance is resolved. This report shall include a description of the event and the corrective or preventative action taken.

- Lists events by date/time range
- Provides drill down to specific events

Motorola Response

Comply.

5.7 Discrepancy Reporting

Errors and discrepancies may occur in any set of data, including databases, configurations, etc. The functional elements and service will support the NENA-STA-010.3 discrepancy report (DR) function. The discrepancy report function is intended to be generated by any entity that is using the data and finds a problem.

Motorola Response

Comply.

- The Discrepancy Reporting web service will be used by a reporting entity to initiate a Discrepancy Report per NENA-STA-010.3.

Motorola Response

Comply.

- Discrepancy Resolution will follow the NENA-STA-010.3 standard to request the resolution to the DR and sends the resolution to the Resolution Uri parameter in the report request.

Motorola Response

Comply.

- Entities will have access to discrepancy status updates.

Motorola Response

Comply.

The Discrepancy Report (DR) function supports a phased response like the following:

- The reporting entity creates the DR and submits it to the responding entity.

Motorola Response

Comply.

- The responding entity acknowledges the DR and provides an estimate of when it will be resolved.

Motorola Response

Comply.

- The reporting entity may request a status update and receive a response.

Motorola Response

Comply.

- The responding entity resolves the DR and reports its resolution to the reporting agency.

Motorola Response

Comply.

All DRs MUST contain common data elements (a prolog) that include:

- Time Stamp of Discrepancy Submittal

Motorola Response

Comply.

- Discrepancy Report ID (a unique value generated by the reporting entity)

Motorola Response

Comply.

- Discrepancy reporting entity FQDN

Motorola Response

Comply.

- Discrepancy reporting agent user ID

Motorola Response

Comply.

- Discrepancy reporting contact info

Motorola Response

Comply.

- Service or Instance in which the discrepancy exists.

Motorola Response

Comply.

-
- Discrepancy Report type (from the list of DRs in this section)

Motorola Response

Comply.

- Additional notes/comments

Motorola Response

Comply.

- Reporting entity's assessment of severity

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Support for NENA-STA-010.3 DR function generated by data users.

Motorola Response

Comply.

Our Discrepancy Reporting Service (DRS) fully conforms to the NENA-STA-010.3 standard and empowers data users to seamlessly generate, submit, and track discrepancy reports via the Discrepancy Reporting API.

Functions Available to Data Users:

- **Report Generation:** Users interacting with the service can actively generate reports for errors discovered in datasets, databases, or configurations. This includes logging specific scenarios like misroutes, incorrect caller locations, and "No Record Found" (NRF) events.
 - **End-to-End Tracking & Visibility:** Once a user generates a report, the API provides them with full transparency, allowing them to track the status of their submission from initiation through to final resolution by the responsible parties.
 - **Dynamic Usability:** Users can easily query for status updates and resolutions to ensure they are informed about discrepancy resolution.
-

- Discrepancy Reporting web service for initiating a DR.

Motorola Response

Comply.

Our Discrepancy Reporting Service (DRS) features a dedicated, secure API specifically designed for authorized users to initiate and manage Discrepancy Reports (DRs).

Web Service Capabilities for Initiating DRs:

- **Seamless Initiation:** Data users and interacting entities can generate and submit DRs directly through the API to communicate errors discovered in NGCS datasets, databases, and configurations.
 - **Comprehensive Scenario Capture:** The API allows users to initiate reports for a wide range of discrepancy scenarios, including misroutes, incorrect caller locations, and "No Record Found" (NRF) events.
 - **Integrated Tracking:** Once a DR is initiated via the web service, users have full visibility, allowing users to track the status of their report from its generation through to final resolution.
-

- Resolution per standard to Resolution URI.

Motorola Response

Comply.

Our Discrepancy Reporting Service (DRS) fully conforms to the NENA-STA-010.3 standard, which includes the proper handling and routing of discrepancy reports to the appropriate Resolution URI.

Resolution Capabilities:

- **Targeted Routing to Responsible Parties:** Discrepancy reports are systematically assigned to the appropriate resolution ownership. This includes the specific parties responsible for the data in error to facilitate accurate tracking and information exchange.
 - **Standardized Resolution Workflow:** The DRS manages the entire lifecycle of the discrepancy, routing the report from its initiation directly to the designated group and posting back the resolution via the resolution URI to the party that initiated it.
-

- Access to status updates.

Motorola Response

Comply.

Our Discrepancy Reporting Service (DRS) provides authorized users with comprehensive, real-time access to status updates throughout the entire lifecycle of a discrepancy. The DRS offers end-to-end status tracking, allowing users to access updates as they happen through the API, with each new status being made available as resolvers actively work through the discrepancy report.

- Phased response (create/submit, acknowledge/estimate, status update, resolve/report).

Motorola Response

Comply.

Our Discrepancy Reporting Service (DRS) manages discrepancies through a structured, phased workflow, providing visibility from initial reporting to final resolution.

Phased Discrepancy Response Capabilities:

- **Create / Submit:** Users can generate and submit discrepancy reports (e.g., misroutes, "No Record Found" events, or location errors) directly through the secure discrepancy reporting API.
 - **Acknowledge / Estimate:** Submitted reports are received and assigned appropriate resolution ownership (e.g., to specific OSP or a dedicated Motorola point of contact). The system systematically logs the effort duration for each participating entity, aiding in the tracking and estimation of resolution timelines.
 - **Status Update:** The DRS actively tracks the status of reports throughout their lifecycle. Authorized users have full transparency to view ongoing status updates and actions taken by responsible parties..
 - **Resolve / Report:** The workflow tracks the issue through to its final resolution by the responsible party. The system maintains a complete transaction history, allowing users to query past discrepancy reports and see the history.
-

- Common prolog elements (timestamp, ID, FQDN, user ID, contact, service/instance, type, notes, severity).

Motorola Response

Comply.

The DRS adheres to the NENA-STA-010.3f standard for both shared fields across discrepancy reports and fields specific to each report type. All fields are validated to ensure they contain appropriate values matching the accepted field types.

5.7.1 Policy and Core Routing

5.7.1.1 Policy Store Discrepancy Report

A client of a Policy Store may report a discrepancy. This type of DR most commonly arises when a Policy Query returns an invalid Policy from the Policy Store. A Policy Owner may retrieve a policy it previously stored to verify the query returns an exact match to the one that was stored; if not, then a DR should be filed against the Policy Store. A policy store may report a discrepancy against itself to raise an issue.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Policy Store DR against Policy Store

Motorola Response

Comply.

The Discrepancy Reporting Service complies with the NENA-STA-010.3f standard for Policy Store discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.1.2 Policy Discrepancy Report

A Policy Discrepancy Report function will be implemented per NENA-STA-010.3. Any entity (such as an ESRP) using a policy (such as a routing policy) will be able to report a discrepancy against the owner of the policy (e.g., a PSAP or an ESRP).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Policy DR against policy owner (e.g., PSAP/ESRP).

Motorola Response

Comply.

The Discrepancy Reporting Service complies with the NENA-STA-010.3f standard for Policy Store discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.1.3 Emergency Services Routing Proxy (ESRP) Discrepancy Report

An ESRP Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. A PSAP or other entity will be able to report a discrepancy against an ESRP when a call is received that should not have been routed to the PSAP, or the ESRP has one or more queues whose fullness is a problem, or if the PSAP seems to be receiving fewer calls than would normally be expected. A routing problem may be the result of incorrect data in the ECRF (GIS data). Calls are sent to PSAPs by ESRPs (Emergency Services Routing Proxy), so a PSAP should report a problem to the ESRP. The ESRP, in turn, reports any suspected GIS problems to the ECRF.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 ESRP DR for misrouted calls, queue fullness, low volume; ESRP reports GIS issues to ECRF.

Motorola Response

Comply.

The Discrepancy Reporting Service complies with the NENA-STA-010.3f standard for ESRP, LoST and GIS discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.2 Location and GIS Sources

5.7.2.1 Location Information Server (LIS) Discrepancy Report

The contractor will include a LIS Discrepancy Report function per NENA-STA-010.3. Any client of a LIS will be able to report a discrepancy.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 LIS DR for LIS clients.

Motorola Response

Comply.

The Discrepancy Reporting Service complies with the NENA-STA-010.3 standard for LIS discrepancy reports.

5.7.2.2 GIS Discrepancy Report

The contractor will include a GIS Discrepancy Report function per NENA-STA-010.3. With this mechanism, the LoST server or other entity will be able to report a discrepancy report against GIS data.

Motorola Response

Comply.

Expected reports include: A gap or overlap discovered when data is coalesced.

- Incorrect information (such as the LoST server to query for information about an area)

Motorola Response

Comply.

- Bad GIS data (such as bad geometry, duplicate attributes, omitted mandatory information, incorrect data type, an address range issue on centerline, a general provisioning failure, or a malformed URI).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 GIS DR for gaps/overlaps, incorrect info, bad data (geometry, attributes, ranges, provisioning, URI).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for GIS discrepancy reports.

5.7.2.3 MSAG Conversion Service Discrepancy Report

A MSAG Conversion Service (MCS) Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. An LSRG or other entity will be able to report a discrepancy against the MSAG Conversion Service (MCS) when a conversion fails, but the querier believes it should have succeeded. A DR may also be filed when the conversion succeeded but the returned location from the MCS is not MSAG-valid or LVF-valid. Both these errors can occur in either direction (PIDF-LO to MSAG or MSAG to PIDF-LO).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 MCS DR for failed conversions or invalid returned locations (PIDF-LO/MSAG bidirectional).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for MCS discrepancy reports.

5.7.2.4 LoST Discrepancy Report

The contractor will include a mechanism for any client of an LVF/ECRF/LoST server to report a discrepancy per NENA-STA-010.3.

The expected reports are:

- The LoST server reports a location as invalid when the client believes it is valid.

Motorola Response

Comply.

- A LIS MAY report a discrepancy against an LVF (as well as against an Originating Service Provider) if a civic address provisioned by an Originating Service Provider for a fixed device is reported invalid by an LVF.

Motorola Response

Comply.

- The LoST server returned an incorrect route in a `findServiceResponse`.

Motorola Response

Comply.

- The LoST server returned an incorrect error or warning regarding the location.

Motorola Response

Comply.

- The `getServiceBoundaryResponse` is incorrect.

Motorola Response

Comply.

- The `listServicesResponse` is incorrect.

Motorola Response

Comply.

- The `listServicesByLocationResponse` is incorrect.

Motorola Response

Comply.

Other discrepancies may be reported but are expected to be less common. These include:

- A client received an address reported as valid that it considers invalid

Motorola Response

Comply.

- Multiple mappings were returned when only one was expected.

Motorola Response

Comply.

- Incorrect service number(s) returned.

Motorola Response

Comply.

- Expired data returned.

Motorola Response

Comply.

- An incorrect <Uri> element was returned.

Motorola Response

Comply.

A DR against a LoST server must also support the ability of the LoST server to report a discrepancy against the GIS data.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Mechanism for LVF/ECRF/LoST client to report discrepancies (invalid location, incorrect route/error/warning, incorrect responses).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for LoST discrepancy reports.

- Support for LIS reports against LVF/OSP.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for LoST discrepancy reports.

- LoST server reports against GIS data.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for LoST discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.3 Signaling and Edge

5.7.3.1 SIP Discrepancy Report

The contractor will have a NENA-STA-010.3 SIP Discrepancy Report function. Entities that encounter an error communicating with another entity via SIP (such as a PSAP) will be able to report a discrepancy.

Motorola Response

Comply.

The expected reports are:

- An initial INVITE request failed.

Motorola Response

Comply.

- A MESSAGE request failed.

Motorola Response

Comply.

- An OPTIONS request failed.

Motorola Response

Comply.

- A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed.

Motorola Response

Comply.

- Required media stream (audio, text, video) failed to be accepted.

Motorola Response

Comply.

- Media problems during a dialog.

Motorola Response

Comply.

- Signaling failure.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 SIP DR for comm errors (failed requests, media stream failures, media problems, signaling failure).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for SIP discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.3.2 Border Control Function (BCF) Discrepancy Report

The contractor will have the BCF Discrepancy Report function as defined in NENA-STA-010.3. This function allows for an entity routing traffic through (to or from) a BCF to report a discrepancy.

The expected reports are:

- Traffic incorrectly blocked before a dialog has been established (e.g., an INVITE, MESSAGE, or OPTIONS request, or response blocked).

Motorola Response

Comply.

-
- Traffic incorrectly blocked during a dialog.

Motorola Response

Comply.

- SIP signaling is inappropriately modified or dropped.

Motorola Response

Comply.

- Session Description Protocol (SDP) incorrectly regenerated during B2BUA/media anchoring.

Motorola Response

Comply.

- Media relayed with loss.

Motorola Response

Comply.

- Traffic permitted that should have been blocked because a designated bad actor generated it.

Motorola Response

Comply.

- Traffic permitted that should have been blocked for some other reason.

Motorola Response

Comply.

- QoS inconsistency.

Motorola Response

Comply.

- Invalid or improper Call Detail Recording.

Motorola Response

Comply.

- TTY to RTT transcoding errors.

Motorola Response

Comply.

- Firewall (non-SIP) errors.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 BCF DR for traffic routing issues (blocked/modified/dropped traffic, SDP regeneration, media loss, permitted bad actor traffic, QoS inconsistency, invalid CDR, TTY-RTT errors, firewall errors).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for BCF discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.4 Network and Infrastructure

5.7.4.1 Network Discrepancy Report

A Network Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. Any entity will be able to report a general networking discrepancy.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 general networking DR.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for Network discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.5 Security and Trust

5.7.5.1 Permissions/Security/Authentication Discrepancy Report

The contractor will deliver a Permissions/Security/Authentication Discrepancy Report function as defined by NENA-STA-010.3. Entities that identify a security issue or a permissions or authentication error that is believed to be incorrect, will be capable of reporting a discrepancy using the DR interface of the entity or element believed to be responsible for the discrepancy.

Motorola Response

Comply.

The expected reports are:

- Unable to authenticate.

Motorola Response

Comply.

- Unable to SUBSCRIBE to an event package.

Motorola Response

Comply.

- Permitted to SUBSCRIBE to an event package when it should have been denied.

Motorola Response

Comply.

- Unable to read a resource.

Motorola Response

Comply.

- Unable to write/modify a resource.

Motorola Response

Comply.

- Unable to delete a resource.

Motorola Response

Comply.

- Able to read a resource when it should have been denied.

Motorola Response

Comply.

- Able to write/modify a resource when it should have been denied.

Motorola Response

Comply.

- Able to delete a resource when it should have been denied.

Motorola Response

Comply.

- Unable to establish secure communication (e.g., TLS certificate is invalid or TLS failure).

Motorola Response

Comply.

- Unable to verify digital signature of a resource (e.g., a routing policy signature verification failed, or the certificate chain is invalid or contains an untrusted authority).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Reports for security/permissions/auth errors (unable to auth/subscribe/read/write/delete, able when denied, TLS/certificate/signature failures).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for Permissions discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.5.2 Log Signature/Certificate Discrepancy Report

A Log Signature/Certificate Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. When an entity (e.g., a Logging Service or another entity) that verifies LogEvent signatures is unable to obtain a certificate, encounters an invalid certificate or thumbprint, or the signature verification fails, it will be able to report the discrepancy to the entity that generated the LogEvent.

Motorola Response

Comply.

The expected cases for this Discrepancy Report are:

- The certificate cannot be obtained (no “x5c” nor “x5u” field provided).

Motorola Response

Comply.

- The “x5u” field cannot be resolved or does not resolve to a valid certificate.

Motorola Response

Comply.

- The “x5u” field is present but the “x5t#256” field is missing, or the thumbprint specified does not match the certificate obtained from the “x5u” field.

Motorola Response

Comply.

- The signature of a LogEvent does not verify.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 report for certificate/signature issues (unobtainable/invalid cert, mismatched thumbprint, failed verification).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for Log Signature discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.6 Data and Logging

5.7.6.1 Logging Service Discrepancy Report

The contractor will have a Session Recording Client (SRC) or any entity generating logging events to, or retrieving logging records from, a Logging Service that may report a discrepancy.

Motorola Response

Comply.

The expected reports are:

- An SRC encountered an error inviting the SRS.

Motorola Response

Comply.

- LogEvent returned an error when it should not have.

Motorola Response

Comply.

- RetrieveLogEvent returned an error when it should not have.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SRC/entity reports for errors in inviting SRS, LogEvent, or RetrieveLogEvent.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for Logging discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.6.2 ADR/IS-ADR Discrepancy Report

An ADR/IS-ADR Discrepancy Report mechanism per NENA-STA-010.3 will be provided. A PSAP, ESRP, ECRF, or other entity or function will be able to report a discrepancy against an ADR or IS ADR.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 ADR/IS-ADR DR by PSAP/ESRP/ECRF/etc.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for ADR discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.7 PSAP Operations and Treatments

5.7.7.1 PSAP Call Taker Discrepancy Report

The contractor will include the ability for a PSAP, downstream agency, or other entity to report a discrepancy against a PSAP Call Taker when a call is received that should not have been transferred to the reporting entity.

Motorola Response

Comply.

The resolution parameter in a DiscrepancyResolution report per NENA-STA-010.3 requires one of the following tokens:

- CallTakerAdvised (the call taker who transferred the call has been advised that the transfer was in error)

Motorola Response

Comply.

- TransferCorrect (the transfer was correct)

Motorola Response

Comply.

- NoDiscrepancy

Motorola Response

Comply.

- OtherResponse

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Reports against PSAP Call Taker for erroneous transfers.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for Call Taker discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

- Resolution tokens (CallTakerAdvised, TransferCorrect, NoDiscrepancy, OtherResponse).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for Call Taker discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.7.2 Call Transfer Failure Discrepancy Report

A Call Transfer Failure Discrepancy Report mechanism will be provided that conforms to NENA-STA-010.3. A PSAP, LSRG, or other entity will be able to report a discrepancy against a transfer entity when a transfer fails. The notification should be made to both the entity originating the transfer and the entity receiving the transfer.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 mechanism for transfer failures, notified to originating/receiving entities.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for Call Transfer discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.7.3 Interactive Media Response (IMR) Discrepancy Report

An Interactive Media Response (IMR) Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. Any entity aware of a discrepancy at an Interactive Media Response (IMR) will be able to report a discrepancy at it.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 IMR DR.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3 standard for IMR discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

5.7.8 External Providers

5.7.8.1 Originating Service Provider Discrepancy Report

A mechanism for Originating Service Providers to file Discrepancy Reports will follow NENA-STA-010.3. The service allows an entity to create a discrepancy against an Originating Service Provider when a location provided by the Originating Service Provider fails validation.

Motorola Response

Comply.

- An ECRF or ESRP or PRF or PSAP may report a discrepancy when a default location is used for routing because the location is missing or not usable.

Motorola Response

Comply.

- An LNG or other entity may report a call received without ANI.

Motorola Response

Comply.

- An LNG or ESRP or other entity may report that a badly formed PIDF-LO was received, or a location query timed out without receiving a PIDF-LO.

Motorola Response

Comply.

- An LSRG or other entity may report that a call was dropped or terminated without appropriate signaling.

Motorola Response

Comply.

- A PSAP may report a discrepancy when a civic location received with a fixed (wireline) call is incorrect.

Motorola Response

Comply.

- A BCF, ESRP, PSAP, or other entity may report an incorrectly formed call (e.g., a SIP INVITE that is badly formed, lacks certain header fields or body parts, etc.).

Motorola Response

Comply.

- A BCF, ESRP, PSAP, or other entity, may report that an unusually large call volume (which might suggest a DoS or other attack) or an unusually low call volume is being generated by the Originating Service Provider.

Motorola Response

Comply.

- An Originating Service Provider may report a discrepancy against itself to raise an issue to be addressed.

Motorola Response

Comply.

- An entity may report a discrepancy when an Additional Data Reference included in the call is invalid.

Motorola Response

Comply.

- An entity may report a discrepancy when an Additional Data value is invalid.

Motorola Response

Comply.

- The Secure Telephone Identity-Verification Service (STIVS) FE may report a Secure Telephone Identity verification failure to an Originating Network.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Mechanism per NENA-STA-010.3 for OSP DRs (invalid/missing location, no ANI, bad PIDF-LO/query timeout, dropped call, incorrect civic, badly formed INVITE, unusual volume, invalid Additional Data, STIVS verification failure).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3f standard for OSP discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies.

- Self-reports by OSP.

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3f standard for OSP discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies

5.7.9 Test and Tools

5.7.9.1 Test Call Generator Discrepancy Report

A Test Call Generator Discrepancy Report mechanism conforming to NENA-STA-010.3 is required. When a Test Call Generator encounters errors initiating or processing a test call, it reports the discrepancy to the PSAP that should have received the test call.

Motorola Response

Comply.

We anticipate incorporating a test call generator into our product development roadmap in the coming months. When test calls are manually generated today, the service automatically logs any discrepancies by monitoring the CHS SIP responses that are automatically generated, e.g., an initial INVITE request failed, a MESSAGE request failed, an OPTIONS request failed, a SIP request sent within a dialog) in response to the NG9-1-1 system's i3 NENA compliant messaging.

The expected cases for this Discrepancy Report are:

- An initial INVITE request failed.

Motorola Response

Comply.

-
- A MESSAGE request failed.

Motorola Response

Comply.

- An OPTIONS request failed.

Motorola Response

Comply.

- A SIP request sent within a dialog (e.g., a re-INVITE or INFO) failed.

Motorola Response

Comply.

- Loopback media stream (audio, text, video) failed to be accepted.

Motorola Response

Comply.

- Loopback media problems during the test dialog.

Motorola Response

Comply.

- Signaling failure.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- NENA-STA-010.3 Test Call Generator DR to PSAP for errors (failed requests, loopback failures, media/signaling issues).

Motorola Response

Comply.

The DRS complies with the NENA-STA-010.3f standard for Test Call discrepancy reports. While machine-generated reports are possible, human-initiated reports are preferred to ensure accurate information for resolving discrepancies

6. Installation Requirements

Respondents are required to assume the primary project management and installation management role for their NG911 system. The State will aid and coordinate support for some aspects of the installation but will be looking for the Respondent (Contractor) to provide all installation services.

Installation as defined in this RFP includes:

- Coordination with PSAPs
- System and service migration (i.e., logging, recording, CAD)
- Coordination with OSPs
 - Ingress
 - Core
 - Egress
- Coordination with current 911 system service provider
 - Ingress
 - Core
 - Egress
- Traffic migration
- Data migration
- Staging
- Testing
- Pre-cutover
- Cutover planning
- Training

The Respondent must, at a minimum, provide installation, maintenance, and support services for the duration of the contract period. Customer service support functions are identified below (§E-9, et seq.) and must be included in the Proposal to ensure that the network is fully supported.

Motorola Response

Comply.

Motorola accepts the role of primary project manager and installation lead for the Nebraska NG9-1-1 system. Our approach ensures a turnkey delivery, where Motorola manages all installation services while collaborating with the State and PSAPs to align with local requirements.

Installation Management and Governance

Motorola provides a dedicated Project Management team to oversee the full lifecycle of the installation. This team serves as the single point of contact for the State, managing timelines, suppliers, and technical coordination across all 9-1-1 stakeholders.

Scope of Installation Services

Our installation methodology addresses every critical layer of the NG9-1-1 ecosystem:

- **Stakeholder Coordination:** We lead the engagement with PSAPs, OSPs, and the current 9-1-1 service provider. This includes managing the technical handoffs at the Ingress (carrier-to-ESInet), Core (NGCS functions), and Egress (ESInet-to-PSAP) points.
- **System and Service Migration:** Motorola manages the integration of essential PSAP services, including Logging/Recording, CAD, and Mapping. We ensure that data migration, including GIS and MSAG transition, is completed and validated prior to live traffic moves.
- **Staging and Testing:** Before onsite deployment, all services are staged in a controlled environment to verify functionality. This is followed by comprehensive **pre-cutover testing** to ensure 100% readiness.
- **Cutover Planning and Execution:** We develop site-specific cutover plans that utilize parallel operations, allowing legacy and NG9-1-1 systems to run simultaneously until the final migration is certified successful.

Maintenance and Long-Term Support

Motorola's commitment extends beyond the initial cutover. We provide full maintenance and support for the duration of the contract, anchored by our NSOC.

Table 5-3: Services and Support

Service Function	Description
24/7/365 Monitoring	Proactive surveillance of all system, device, and application-level faults.
Fault Remediation	Immediate remote or onsite response to system-impacting events based on defined SLAs.
Patch & Virus Management	Regular deployment of validated security patches and antivirus updates to maintain system integrity.
Disaster Recovery	Automated backups and snapshots to ensure operational continuity in the event of major failures.

Training

Motorola delivers a training program tailored to Nebraska's needs. This includes curricula for technical training for IT staff on system administration and troubleshooting.

6.1 Installation Services

The Contractor is responsible for the installation of all requirements listed in the RFS and attachments and any other functional elements such as power and UPS as necessary to implement their NG911 solution. Devices that are installed at a PSAP may require analysis of the power and backup power supply at that PSAP. In some cases, the contractor may need to remediate issues to ensure their device has the resources needed. The State may aid coordination support for some aspects (such as approvals and scheduling) of the installation but is relying upon the Contractor to perform all installation services.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Methodology for installation of all NG911 system components and explain the approach to completing installation of the delivery of NG911 traffic. The methodology must include coordination with OSPs, PSAPs and other potential networks that can enhance the delivery of 911 traffic across the system.
- Coordination methodology to interconnect with all current telecommunication companies that are responsible for 911 call delivery and explain how these providers are accounted for during implementation.
- Plan to coordinate with all current 911 system service providers.
- Installation services to be provided and outline the roles and responsibilities of the Contractor and Subcontractor(s) during installation. Installation tasks as defined include, but may not be limited to:
 - Coordination with PSAPs
 - System and service migration (i.e., logging, recording, CAD)
 - UPS integration to support a minimum 3-hour backup validated with an MTTR / MTBF calculation
 - Coordination with OSPs
 - Coordination with current 911 system service provider
- Traffic migration
- Data migration
- Staging
- Acceptance testing
- Cutover planning
- Training

Motorola Response

Comply.

Motorola assumes full accountability for the turnkey installation of the Nebraska NG9-1-1 solution. Our methodology prioritizes service continuity, ensuring that every transition point, from power at the PSAP to the core network, is managed with precision.

Installation and Traffic Delivery Methodology

Motorola utilizes a **phased integration approach** to move 9-1-1 traffic from legacy networks to the i3-compliant ESInet.

OSP and Network Interconnection: We coordinate directly with all OSPs and adjacent networks. For providers not yet IP-capable, we deploy LNG to aggregate and convert TDM traffic into SIP, ensuring comprehensive coverage from day one.

PSAP Readiness: Our teams perform comprehensive site surveys at each PSAP to assess power, space, and environmental conditions. This includes the integration of UPS systems designed to support a minimum 3-hour backup. We validate these systems using MTTR and MTBF calculations to ensure long-term reliability.

Note: Motorola is not proposing or pricing UPS hardware at each NGCS integration point (PSAP host sites/NGCS demarcation sites). NGCS hardware at these sites will utilize available, clean redundant power sources. Site surveys will identify space and power requirements for each site.

Coordination with Incumbent Providers and Carriers

Motorola manages the complex interface between the new ESInet and existing infrastructure:

- **Telecommunications Coordination:** We map every existing trunk and circuit from current providers. During implementation, these providers are treated as critical dependencies in our project schedule, with dedicated technical leads assigned to manage the handoff.
- **Incumbent Provider Collaboration:** We establish a formal joint-operating agreement with the current 9-1-1 service provider to manage the **Ingress, Core, and Egress** transitions. This ensures that as traffic is migrated, routing logic remains synchronized between the old and new systems.

Installation Roles and Responsibilities

Motorola serves as the prime contractor, maintaining oversight of all suppliers to ensure a single point of accountability.

Table 5-4: Roles and Responsibilities

Task	Primary Responsibility	Description
Project Management	Motorola	Overall schedule, stakeholder coordination, and risk mitigation.

Task	Primary Responsibility	Description
Site Surveys & UPS	Motorola	Analysis of PSAP power/backup; remediation of power issues.
Data Migration	Motorola / GIS Lead	Transition of MSAG/ALI data to the new SI.
Traffic Cutover	Motorola	Phased migration of live 9-1-1 traffic with parallel operation.
Training	Motorola	Comprehensive curricula for admin and PSAP personnel.

Execution Phases

- **Pre-Cutover:** We finalize "as-built" documentation and perform end-to-end testing with the PSAPs' peripheral services (CAD, Logging Recorders).
- **Traffic & Service Migration:** We execute a site-by-site cutover. Each migration includes a **Go/No-Go checkpoint** and a pre-validated rollback plan to ensure 9-1-1 services are never interrupted.

6.2 Wiring and Cabling

All interface connections and visible cables must use standard EIA connectors secured by wall plates where exposed. All cables must be clearly marked and/or numbered in a manner that reflects a unique identifier of the cable at both ends. Any cables used must be plenum rated where required by local building or fire codes.

Respondents must ensure that all equipment is connected to emergency AC power and is configured to be supported by a UPS.

Motorola Response

Comply.

Early in the implementation process we will work with each location where NGCS equipment will reside to identify clean and safe power requirements and action plans for the PSAP to resolve any deficiencies.

Assumption Regarding UPS Provisioning: We assume that each participating PSAP will provide a suitable UPS infrastructure with adequate capacity to support the proposed hardware. Should a PSAP lack the available UPS capacity, or if the existing UPS is deemed to be inadequate to support the new equipment, any required UPS upgrades, electrical modifications, or new installations, are explicitly outside the scope of Motorola's responsibility and must be procured and provisioned by the respective PSAP.

Cabling, communications outlets, power wiring, system grounding, conduit facilities, and equipment rooms must be installed in accordance with national standards and applicable local codes.

Motorola Response

Comply.

Early in the implementation process we will work with each location where NGCS equipment will reside to identify action plans for the PSAP to resolve any deficiencies prior to hardware installation.

The minimum standards used in the installations shall include, but are not limited to, the following:

- ANSI/TIA/EIA-568 – Commercial Building Telecommunications Wiring Standard

Motorola Response

Comply.

- ANSI/TIA/EIA-569 – Commercial Building Standard for Telecommunications Pathways and Spaces

Motorola Response

Comply.

Early in the implementation process we will work with each location where NGCS equipment will reside to identify action plans for the PSAP to resolve any facility deficiencies prior to NGCS HW installation.

- ANSI/TIA/EIA-606 – Administration Standard for the Telecommunications Infrastructure of Commercial Buildings

Motorola Response

Comply.

Early in the implementation process we will work with each location where NGCS equipment will reside to identify action plans for the PSAP to resolve any deficiencies prior to NGCS HW installation.

- ANSI/TIA/EIA-607 – Commercial Building Grounding and Bonding Requirements for Telecommunications

Motorola Response

Comply.

Early in the implementation process we will work with each location where NGCS equipment will reside to identify action plans for the PSAP to resolve any deficiencies prior to NGCS HW installation.

- Building Industry Consulting Service International, Telecommunications Distribution Methods Manual

Motorola Response

Comply.

- National Electrical Code (NFPA-70)

Motorola Response

Comply.

- FCC Rules and Regulations, Parts 68 and 15

Motorola Response

Comply.

6.3 Grounding

The proposed system must provide surge and lightning protection for all connections to AC power and is required to meet the R-56 standard.

Motorola Response

Comply.

All hardware and peripheral devices must be mechanically and electrically grounded to prevent both user hazard and loss of data or hardware integrity due to external electrical impulse.

Motorola Response

Comply.

Respondents must ground all equipment in compliance with manufacturer recommendations and applicable standards.

Motorola Response

Comply.

Respondents must furnish and install the required grounding and bonding conductors where necessary and complete the connections to the grounding system at all sites.

Motorola Response

Comply.

7. Training

The Respondent shall work cooperatively with the State and designated staff to deliver training for the proposed solution. Training shall be ongoing throughout the term of the contract, with the ability to provide on-demand sessions at the State's request. The Respondent must include a description and supporting documentation for all requirements in this section.

Motorola Response

Comply.

Motorola provides the VESTA NXT Router as a fully managed **Service**, which minimizes the technical burden on State and PSAP personnel. In this approach, the complex management, 24/7 monitoring, and maintenance of the ESInet and NGCS are handled directly by our NSOC.

Service-Based Training Approach

Because Motorola maintains end-to-end accountability for system performance, training is streamlined to focus on the essential touchpoints where Nebraska personnel interface with the service environment:

- **Service Interface Training:** Instruction is focused on processes for interacting with the NSOC, including incident reporting, service requests, and accessing real-time status dashboards.
- **Operational Simplicity:** As the underlying i3 FEs (ESRP, ECRF, BCF) are managed as a service, local staff are relieved of deep technical system administration, significantly reducing the training hours typically required for legacy hardware.

Commitment to Nebraska's Requirements

Regardless of this streamlined service model, **Motorola will provide whatever training and materials the State feels are necessary for the VESTA NXT Router Service.** We remain fully committed to ensuring that all State and PSAP personnel feel confident in their understanding of the system's

operation. We will work cooperatively with the State to customize curricula, documentation, and session frequency to meet your specific operational standards and comfort levels.

7.1 Audiences and Scope

PSAP Operations:

- Network status reports
- Help desk usage and processes
- Text-to-911 operations
- Text- from-911 operations
- Trouble Ticketing

State-Level Operations:

- Network status reports
- Help desk processes
- Trouble ticketing
- Root-cause analysis and review

Motorola Response

Comply.

Motorola's operational framework is designed to provide transparent, real-time visibility and support tailored to both local PSAP needs and statewide strategic oversight. We utilize a tiered support structure anchored by our 24/7/365 NSOC.

PSAP Operations Support

Motorola provides local agencies with the tools and information necessary to manage daily emergency communications with confidence:

- **Network Status Reports:** PSAPs receive localized dashboards and automated alerts. These reports provide immediate visibility into the health of their specific ESInet connection and FEs.
- **Help Desk Usage and Processes:** PSAP personnel have direct access to our 9-1-1 specialized help desk. We provide a simplified intake process via phone, email, or web portal, ensuring that front-line dispatchers can report issues without navigating complex menus.
- **Text-to-911 and Text-from-911 Operations:** Training associated with managing Text-to-911 and Text-from-911 and the associated workflows would be included with the call handling solution. This type of training would typically cover the initiation of outbound texts (Text-from-911) for dropped calls and the handling of inbound emergency sessions within the call-handling interface.

- **Trouble Ticketing:** PSAPs can open, track, and view the status of their own tickets. Automated notifications keep the reporting agency informed of estimated restoration times and technician assignments.

State-Level Operations and Oversight

For State leadership, Motorola provides a macro-view of the Nebraska NG9-1-1 ecosystem to ensure contract compliance and systemic health:

- **Statewide Network Status:** A "Manager of Managers" (MoM) dashboard provides the State with a real-time map of the entire ESInet, highlighting regional trends, OSP ingress health, and core NGCS performance.
 - **Aggregate Help Desk & Ticket Analytics:** The State receives monthly reports detailing help desk performance, including average speed to answer, ticket volume by category, and MTTR across all PSAPs.
 - **Trouble Ticketing Governance:** State administrators have "super-user" access to the ticketing system, allowing them to monitor high-priority incidents statewide and ensure SLAs are consistently met.
 - **Root-Cause Analysis (RCA) and Review:** For any Priority 1 or systemic incident, Motorola conducts a formal RCA. These reports identify the primary failure point, the effectiveness of the response, and the permanent corrective actions taken to prevent recurrence. These are presented to the State for formal review and sign-off.
-

7.2 Training Elements

The Respondent shall develop and deliver training to meet the following minimum requirements:

- Login and logout procedures
- Password reset
- Equipment problem reporting
- Call transfer functionality
- Call conferencing functionality
- Discrepancy reporting
- Foreign language interpretation process
- Rebid/refresh of call information
- Instant recorder/playback
- Text-to-911
- Text-from-911
- Other solution features not otherwise listed

Motorola Response

Comply.

Motorola's training program ensures that all Nebraska applicable staff is proficient in both the foundational and advanced features of the NG9-1-1 system.

7.3 Technical Assistance

Upon request by the State, the Contractor shall provide technical assistance to PSAP personnel during training and testing.

Motorola Response

Comply.

Motorola provides dedicated, technical assistance to ensure Nebraska PSAP personnel feel confident and supported during the critical windows of Testing and Training. We recognize that the transition to a NENA i3 architecture involves a significant shift in workflow, and our technical teams are structured to provide immediate, hands-on guidance.

7.4 Schedule and Locations

No later than fourteen (14) calendar days before each PSAP cutover, train all PSAP personnel (including State and administrative personnel assigned to the PSAP) on the proper operation of all Contractor-supplied software and equipment. To maintain the deployment schedule and accommodate call-taker travel, the Contractor shall establish temporary training site(s) in Nebraska as needed and provide weekend and evening sessions when required.

Motorola Response

Comply.

Motorola is committed to a flexible, localized training strategy that minimizes operational disruption for Nebraska's PSAPs while ensuring 100% staff readiness. We acknowledge and will comply with the requirement to complete all training no later than 14 calendar days prior to each individual PSAP cutover.

7.5 Training Materials

Provide all training materials and a Train-the-Trainer (TtT) curriculum for State approval. Maintain up-to-date training materials at the State for the duration of the contract.

Motorola Response

Comply.

7.6 Post-Deployment Training and Costs (Proposal Requirement)

The Respondent shall, as part of their response:

- Provide a proposed cost for post-deployment training for up to fourteen (14) students per class
- Provide a proposed cost for the post-deployment TtT course, including the maximum class size.

Motorola Response

Comply.

Motorola has provided pricing for all post-deployment training scenarios within the **Cost Proposal** section of this response, including:

- **Post-Deployment Student Training:** Pricing for standardized courses accommodating up to **14 students per class**.
- **Train-the-Trainer (TtT) Course:** Pricing for the TtT certification program with a maximum class size of **10 students** to ensure instructional mastery.

While the **VESTA NXT Router** is delivered as a Service with minimal operational overhead, Motorola remains fully committed to the State's educational requirements. Regardless of the service-based nature of this solution, we will provide additional training sessions or specialized materials the State deems necessary to ensure personnel are fully comfortable with the VESTA NXT Router Service.

7.7 Comprehension, Testing, and Certification

Apply testing at intervals during initial and ongoing training and provide the State a final evaluation of each student's knowledge upon completion. Instructional methodologies shall include lectures, group discussions, audiovisual methods, and role-playing. Testing methodologies shall include written exams, oral exams, hands-on testing, and end-of-course certification.

Motorola Response

Comply.

7.8 Training Plan and Samples (Proposal Requirement)

The Respondent shall, as part of their response:

- Provide a proposed training plan and sample documentation and/or materials covering the topics and audiences listed in §E-8.1 and §E-8.2, above.

Motorola Response

Comply.

A Training Plan is included within our Sample Project Management Plan, found in Exhibit 4, Section 4.

8. Operations and Service Management Requirements

The Contractor shall manage all service support for the NG911 system, including integration of service and support for all partners and Subcontractors delivering components to the State.

Motorola Response

Comply.

Service levels and escalation: The Contractor shall commit to 99.999% availability for core voice paths, MTTR < 2 hours for Priority 1 incidents, and defined response times (for example, 15-minute acknowledgment). Include documented escalation paths, root-cause analysis reports, and penalty provisions for SLA breaches.

Motorola Response

Comply.

Our NGCS and ESInet are backed by comprehensive SLAs that define availability, aggressive response times, automated escalations, and concrete financial penalties to guarantee absolute accountability.

- **99.999% Availability & MTTR:** We commit to a 99.999% Service Availability SLA for Call Routing, permitting a maximum downtime of just 5.26 minutes annually. Priority 1 incidents are bound by a 15-minute target response time, hourly status updates, and a strict MTTR of under 2 hours.

- **Automated Escalation Paths:** Automated SLA timers trigger immediate escalations based on elapsed response time: 50% (Assigned Engineer), 75% (Manager), and 100% (Sr. Manager of Technical Service Delivery). Unresolved critical issues are escalated up to the Director of NGCS Operations and are managed via a continuous emergency incident bridge until resolution.
 - **Root-Cause Analysis (RCA):** Following a critical outage, we provide a preliminary Event Analysis Report (EAR) within 3 to 5 business days. A comprehensive Final RCA—detailing the exact timeline, root cause, and preventative actions—is delivered within 10 to 30 calendar days.
 - **Financial Penalty Provisions:** Information regarding service credits associated with SLAs are included in Exhibit 9 Service Level Agreements.
-

Operations enablement:

Provide comprehensive training curricula (in-person and virtual), role-based certifications, and operational runbooks for common scenarios such as failover and GIS updates. Supply full technical documentation that uses NENA functional-element nomenclature and is tailored to PSAP operators, network administrators, and GIS staff.

Motorola Response

Comply.

Change management:

Establish documented change-control protocols, including scheduled maintenance windows during off-peak hours, rollback procedures, impact assessments, and at least 30 days' advance notice for changes that affect routing, GIS, or call handling.

Motorola Response

Comply.

Standards conformance and interoperability:

Demonstrate conformance to NENA i3 and NGCS standards through self-attestation and participation in multi-vendor interoperability events (for example, NENA ICE). Test plans shall include NENA-defined sequences, and the system shall interoperate with third-party equipment (for example, CHE from different vendors).

Motorola Response

Comply.

Testing program:

Execute a phased testing program covering unit tests, component integration, system integration, failover simulations, performance, and load testing (including 200% of peak capacity), and security validations using NENA test cases. Success criteria shall include 100% pass rates for critical flows.

Motorola Response

Comply with Clarification.

We comply with all requirements. Validation testing will instead utilize the NG9-1-1 Interoperability Task Force test cases instead of NENA test cases.

Product documentation:

Provide thorough user manuals, API specifications (in OpenAPI format), and release notes, along with the training programs noted above, aligned with NENA terminology.

Motorola Response

Comply.

8.1 Service Management Framework

8.1.1 Service Management Plan

Oversight of the NG911 system and services post implementation/transition is required. The preferred best practice is to utilize Information Technology Infrastructure Library (ITIL) as a guideline for how NG911 services are designed, implemented, managed, maintained, and improved within the term of the contract.

Motorola Response

Comply.

Details concerning our support is provided in Exhibit 10 Sample Support Plan.

ITIL integrates five stages of service delivery into a comprehensive methodology for managing the lifecycle of services.

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Motorola Response

Comply.

Within these stages are specific areas relating to Information Technology Service Management.

At a high level, these areas reference how a service maintains availability, capability, capacity, security, manageability, and operability. Respondents must describe their approach to service management for the operation of the NG911 system. The NG911 service management approach shall incorporate components of ITIL or follow industry best practices for IT service management.

Motorola Response

Comply.

We deliver an end-to-end, ITIL-aligned service management program powered by our enterprise ServiceNow platform. This proven framework guarantees rapid incident resolution, transparent communication, and zero-disruption system maintenance for your NG9-1-1 environment.

- **24x7x365 NSOC:** Serving as your central hub for continuous monitoring and incident management, the NSOC immediately logs, triages, and escalates all user-reported issues and automated system alerts to ensure rapid resolution within strict SLAs.
 - **Dedicated CSM:** This role serves as your primary liaison and escalation point, overseeing the daily lifecycle of your service, managing critical incident updates, and acting as your dedicated Change Manager.
 - **Strict ITIL Change Management:** To completely prevent disruptions to day-to-day operations, all system updates, security patches, and network modifications require a formal service change request. Every change mandates a rigorous impact assessment, an executable rollback plan, explicit Change Advisory Board (CAB) approval, and a formal Post Implementation Review (PIR).
 - **Transparent CWP:** We provide your authorized personnel with direct, secure access to our ITSM platform. This portal delivers near real-time visibility into network health, active incident ticket progression, and all scheduled Change Management events.
-

Respondents must provide a narrative of how their proposed service management approach is integrated into their project management activities. Respondents must discuss their ability to maintain consistent performance and the service levels of the network

Motorola Response

Comply.

Motorola embeds service leadership directly into the project lifecycle to guarantee a flawless transition from implementation to day-to-day operations, while maintaining uncompromising network performance through resilient architecture and proactive monitoring.

Seamless Project-to-Operations Transition

- **Early Operational Engagement:** A dedicated CSM is assigned during the project phase to define and refine support policies, ensuring all SLAs are formally validated and aligned prior to the system going live.
- **Unified ITIL Change Management:** We utilize the exact same ServiceNow-driven ITIL framework during both implementation (to manage scope/schedule changes) and live operations (to manage maintenance and upgrades), ensuring absolute consistency.
- **Structured NSOC Handover:** Following successful cutover and acceptance testing, the Project Manager transitions comprehensive network and configuration documentation directly to the 24x7x365 NSOC to ensure immediate operational readiness.

Consistent Performance & SLA Enforcement

- **99.999% Operational Availability & Sub-Second Reconvergence:** Engineered with zero single points of failure, our ESInet guarantees 99.999% Operational Availability. We leverage dynamic routing protocols (OSPF, BGP) and Fast Reroute (FRR) technologies to deliver sub-second failover, ensuring active calls are never dropped during a network event.
 - **Strict QoS & Proactive Monitoring:** The NSOC continuously monitors system health and historical trends to remediate anomalies proactively. We enforce strict QoS to prioritize voice traffic, guaranteeing a daily Predicted Mean Opinion Score (PMOS) of 3.5 or higher for audio clarity.
 - **Automated Escalation & Full Transparency:** ServiceNow automatically triggers SLA escalation timers the moment an issue is detected. Your agency retains near real-time visibility into all network nodes, bandwidth utilization, call routing activity, and SLA compliance reporting via the secure CWP.
-

Respondents must discuss their ability to maintain consistent performance and the service levels of the network to support the following framework:

- Determination of the single point of contact

Motorola Response

Comply.

We provide consistent network performance and strict SLA adherence by establishing clear, unwavering lines of communication and accountability through a defined Single Point of Contact framework.

- **Dedicated CSM:** This role acts as your primary administrative liaison and strategic single point of contact throughout the lifecycle of the service.
-

- Management of subcontracted support components

Motorola Response

Comply.

We assume prime contractor accountability for your entire NG9-1-1 ecosystem. We seamlessly manage all subcontracted vendors and third-party support components behind the scenes, ensuring you receive a unified, frictionless service experience governed by our strict standards.

- Support personnel required and identification of Key Personnel

Motorola Response

Comply.

Motorola provides a comprehensive, multi-tiered support structure to ensure continuous, zero-disruption 9-1-1 operations. We formally designate Key Personnel who remain dedicated and accountable to your agency from initial implementation through long-term day-to-day operations.

Table 5-5: Dedicated Key Personnel

Role	Lifecycle Phase	Primary Responsibilities
Project Manager	Implementation	Serves as the deployment single point of contact, manages SATP/FATP acceptance testing, and executes the formal transition handover to the NSOC.
Customer Service Manager	Ongoing Operations	Acts as your strategic administrative liaison, oversees daily SLA compliance, leads the Change Advisory Board (CAB), and conducts operational reviews.
Incident Manager	Active Outages	Assumes absolute, single-threaded ownership during Critical (Priority 1) events, mobilizing resources 24x7x365 until full service restoration is achieved.

- Underpinning contract management

Motorola Response

Comply.

We guarantee that all underpinning contracts with our third-party vendors and network providers strictly mirror our prime contract commitments. This legally binds our supporting ecosystem to the exact same 99.999% Operational Availability guarantees, (Priority 1) response times, and aggressive MTTR targets.

- Third-party support contracts

Motorola Response

Comply.

We assume total prime contractor responsibility for all third-party support contracts required to deliver your NG9-1-1 solution. We completely shield the State from the administrative burden of multi-vendor management, ensuring all external contracts seamlessly support our overarching service guarantees.

- Pre-emptive support

Motorola Response

Comply.

We ensure continuous NG9-1-1 availability by shifting from reactive troubleshooting to a highly proactive, pre-emptive support model. Driven by advanced AI, continuous network polling, and rigorous preventive maintenance, we identify and neutralize potential issues before they impact live operations.

- Equipment refreshes

Motorola Response

Comply.

We proactively manage the modernization of the NG9-1-1 ecosystem through a guaranteed hardware and software lifecycle refresh program, ensuring your architecture remains highly stable, secure, and fully aligned with evolving industry standards.

- Preventative maintenance

Motorola Response

Comply.

We ensure the continuous reliability and security of your NG9-1-1 ecosystem through a rigorous, ITIL-governed preventative maintenance program designed to identify and resolve potential issues long before they impact live operations.

We require routine, scheduled maintenance and rigorous health checks on all critical infrastructure including core network devices, servers, and precision master clocks to proactively prevent isolation or unexpected component failure.

- Bug fixes

Motorola Response

Comply.

We ensure the continuous reliability and security of your NG9-1-1 software through a rigorous, ITIL-governed defect resolution process. We identify, test, and deploy bug fixes swiftly with zero disruption to your live operations.

Software defects are immediately logged in our centralized ServiceNow ITSM platform and triaged by our 24x7x365 NSOC). Bugs are categorized by severity, ensuring critical defects are aggressively managed under our SLA.

- Patching and upgrades

Motorola Response

Comply.

We provide a secure, fully optimized, and NENA i3-compliant NG9-1-1 ecosystem through a rigorous, ITIL-governed patching and upgrade process designed specifically to eliminate downtime and protect live operations.

All security patches, firmware updates, and system upgrades are strictly controlled via our ITIL Change Management framework. Every update requires a formal service change request, thorough risk assessment, explicit Change Advisory Board (CAB) approval, and a fully executable rollback plan before being applied to the production environment.

- Warranty

Motorola Response

Comply.

We act as the single prime contractor, directly holding, negotiating, and executing all underlying Original Equipment Manufacturer (OEM) warranties and third-party support contracts. We completely shield the State from multi-vendor warranty disputes or "finger-pointing."

- Out of warranty items

Motorola Response

Comply.

Because we deliver the NGCS/ESInet solution as a continuously managed service, no contracted core hardware or software component will ever fall out of warranty. We hold and maintain all underlying Original Equipment Manufacturer (OEM) support contracts behind the scenes.

- Service Level Agreements

Motorola Response

Comply.

Per the RFP requirement, we will negotiate a comprehensive SLA framework that defines specific, measurable, achievable, relevant, and time-bound (SMART) metrics for the performance, availability, and reliability of the ESInet and all its FEs with the State.

8.1.2 Service Level Agreement (SLA)

The NG911 system will utilize the requirements outlined in this RFP to negotiate a Service Level Agreement (SLA) with the selected vendor. In preparation all Respondents must provide a description of their SLA performance measures and identify how the thresholds that are not met are recovered.

The Respondent shall negotiate a comprehensive Service Level Agreement (SLA) framework that defines specific, measurable, achievable, relevant, and time-bound (SMART) metrics for the performance, availability, and reliability of the ESInet and all its functional elements. This framework must detail the processes for monitoring, reporting, and reviewing SLA compliance. The approach should align with industry best practices for IT service management and project management to ensure consistent quality and continual improvement.

The State expects the Respondent to provide a description of how each of these components are met within their SLA.

The State recognizes the following categories as expectations for their SLA.

Critical – Network Outage

- 1st Level Support – Immediate
- Continuous problem resolution/workaround effort
- 2nd Level Support – within 15 minutes
- 3rd Level Support – within 30 minutes or upon Customer request.

Major – Service effecting

- 1st Level Support – Within 5 minutes
- 2nd Level Support – Within 30 minutes
- 3rd Level Support – Within 2 Hours or upon Customer request.

Minor – Non-service effecting

- 1st Level Support – Within 30 minutes
- 2nd Level Support – Within 2 Hours
- 3rd Level Support - Within 1 business day or upon Customer request.

The Respondent must provide a description and/or documentation that supports the requirements in this section.

Motorola Response

Comply.

Per the requirements outlined in this RFP, Motorola welcomes the opportunity to negotiate an SLA agreement with the Commission. Below and provided in Exhibit 9 you will find our standard SLA framework:

We categorize service incidents into four distinct severity (or priority) levels within its SLAs and support plans. These categories dictate the required response times, communication intervals, and escalation procedures:

- **Critical (Level 1 / Priority 1):** This category is defined as a full loss of critical functionality, meaning the service or its critical components are completely inoperative. Examples include a total service failure, a network outage preventing communications with the PSAP, or the inability to route 9-1-1 calls to a valid destination.
 - **Target Response Time:** Within 15 minutes.
 - **Communication Interval:** Hourly updates.
 - **High (Level 2 / Priority 2):** This category involves a significant degradation or partial loss of critical functionality, but a workaround may be available. Examples include an intermittent service failure, loss of two or more OSP ingress networks, or a 50% loss of the IP network to the PSAP.
 - **Target Response Time:** Within 30 minutes.
 - **Communication Interval:** Updates every 2 hours.
 - **Medium (Level 3 / Priority 3):** This is defined as a minor degradation of service functionality or capacity that does not have a serious impact on 9-1-1 call delivery. Examples include the loss of a non-critical system component, a failure impacting only a single position, or an error condition where a workaround has already been determined.
 - **Target Response Time:** Within 4 hours.
 - **Communication Interval:** Daily updates.
 - **Low (Level 4 / Priority 4):** This category is used for informational requests, general questions, or minor/cosmetic impairments that do not negatively impact inbound call processing. Examples include reporting formatting issues or non-service affecting system anomalies.
 - **Target Response Time:** Next business day.
 - **Communication Interval:** Updates provided as needed via email or the CWP.
-

8.1.3 Compliance and Risk Management

The State requires the contractor to run a documented risk management program for all NGCS components and the ESInet. The program must identify assets, threats, and vulnerabilities; rate and rank risks by **likelihood** and **impact** on **call delivery, location accuracy, security, availability, latency, and resilience**; and select a treatment (reduce, avoid, transfer, or accept). Any non-compliance with security requirements, standards, procedures, or practices must be documented and submitted to the State for written approval, including criticality analysis and a corrective action and/or risk acceptance path.

Motorola Response

Comply.

Motorola employs a comprehensive and documented risk management program for all NGCS components and the ESInet, anchored in the NIST Cybersecurity Framework and NENA i3 standards, among other relevant industry standards and best practices. Our approach begins with a rigorous asset identification process that catalogs every functional element of the system—from ECRF to physical hardware and cloud resources. This inventory serves as the foundation for our continuous threat and vulnerability assessment lifecycle, where our centralized Cybersecurity Team utilizes the automated scanning to detect emerging risks. Each identified vulnerability is rated and ranked based on its potential impact on critical performance requirements. By quantifying the likelihood of occurrence against these mission-critical benchmarks, Motorola ensures that our emergency communications infrastructure is protected by a data-driven security posture.

Once risks are identified and ranked, we apply a formal treatment methodology to manage them effectively. Every risk is addressed through a specific strategy to either reduce the threat via technical mitigations, avoid it through architectural changes, transfer it through managed service guarantees, or accept it if it falls within the State's pre-defined tolerance levels. This lifecycle management extends to our sourcing practices, where we maintain strict supply chain oversight to ensure that all hardware and software components meet public-safety grade requirements. By integrating managed detection and response with proactive infrastructure audits, we eliminate the need for costly "rip and replace" cycles, instead providing a path for continuous evolution and hardening of our infrastructure and applications against evolving cyber threats.

Transparency and accountability are central to our partnership with our end customers, particularly regarding compliance and remediation. In the event that any component or practice deviates from established security requirements, we provide a comprehensive criticality analysis that documents the non-compliance in detail. This includes a clearly defined corrective action plan or a formal risk acceptance path.

Each risk under the contractor's control or those outside of the contractor's span of control that will negatively impact the ESInet or NGCS must be recorded on a risk acceptance form and signed by a member of the contractor's senior leadership with the authority – and financial/legal responsibility – to accept that risk for the NGCS/ESInet scope.

Motorola Response

Comply.

All risks must be reassessed at least annually, and high/critical risks at least monthly. The method may use qualitative (very low ↔ very high) or numeric scales but must address both likelihood and impact.

Motorola Response

Comply.

Third-party risks (carriers, cloud providers, data suppliers, managed services, subcontractors) must be tracked and visible even when control is limited. Where a third-party risk could affect service to the State, the contractor must implement compensating controls and define escalation tied to SLA/SLOs (e.g., uptime, MTTR).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- A documented Risk Management methodology covering asset identification, threat identification, vulnerability assessment, risk assessment and prioritization, and risk treatment selection (reduction, avoidance, transfer, acceptance). Include working definitions of threat, vulnerability, and risk, and show how business impact is mapped to NGCS/ESInet outcomes (call completion, routing location, latency, availability).

Motorola Response

Comply.

We ensure the continuous protection of your NG9-1-1 ecosystem by aligning our cybersecurity framework with strict industry standards (NIST SP 800-30/53, ISO 27001/31000). Our methodology operates on the principle that security and system availability must be planned together to ensure their respective impact zones perfectly align.

Core Definitions & Risk Treatment

To maintain absolute clarity in our security operations, we calculate and categorize risk using explicit terminology:

- **Threat:** Any event with the potential to adversely impact operations, assets, or personnel through unauthorized access, destruction, or denial of service.
- **Vulnerability:** A specific weakness in a system, internal control, or architecture that a threat source could exploit.
- **Risk:** The calculated measure of the likelihood of a threat exploiting a specific vulnerability, combined with the resulting operational or financial impact.

Upon identifying a risk, our security engineering teams actively manage it by executing one of four specific treatment strategies:

- **Reduction (Mitigation):** Implementing advanced controls (e.g., IDS/IPS, strict access controls) to decrease the risk's likelihood or impact to an acceptable level.
- **Avoidance:** Eliminating the hazard entirely, such as disabling a vulnerable legacy protocol or halting a high-risk operational activity.
- **Transfer:** Shifting the financial or operational burden to a designated third party, such as offloading infrastructure risks to our Tier 4 data center partners.

- **Acceptance:** Formally acknowledging and monitoring a risk without adding controls, strictly used only when the calculated risk falls well within the agency's predefined risk appetite.

NIST-Aligned Risk Methodology

- **Asset & Threat Identification:** Our 24x7x365 NSOC leverages advanced SIEM tools, IDS/IPS, machine learning algorithms, and external intelligence (Public Safety Threat Alliance) to continuously hunt for anomalous traffic patterns.
- **Vulnerability Assessment:** Aligned with NIST SP 800-30, we conduct deep threat analyses and execute mandatory vulnerability scans upon initial deployment, following any major system change, and annually.
- **Proactive Mitigation:** We minimize our attack surface through Zero Trust architecture, Principle of Least Privilege access, DISA STIGs system hardening, and dedicated DDoS/TDoS countermeasures.

Business Impact Mapped to NGCS Outcomes

We map business risk and severity directly to how an event impacts core NG9-1-1 outcomes, formalized through our SLAs:

- **Call Completion & Location Delivery:** Any failure that stops the routing of 9-1-1 calls or degrades associated location processing (ANI/ALI) with no workaround is immediately classified as a Critical (Priority 1) business impact, violating our 99.999% Operational Availability SLA.
- **Network Performance & Voice Quality:** Latency, jitter, and packet loss are strictly controlled to protect audio clarity. If network degradation causes the daily PMOS to fall below 3.5, or if egress MOS degrades by more than 0.2 from ingress, it triggers a severe business impact resulting in SLA financial penalty credits.

- A risk register template and sample entries showing fields for asset, threat, vulnerability, likelihood, impact, inherent and residual risk, selected treatment, owner, due dates, status, and verification of closure. Include examples for both NGCS applications and ESInet network elements.

Motorola Response

Comply.

Here is an example of our current risk register template. Upon award, Motorola will work with the State to develop mutually agreed upon forms and templates required to support the State of Nebraska deployment and ongoing support of the project.

RISK REGISTER									
ID	Risk Category	Risk Identified Date	Risk Identified By	Risk Description	Risk Action Plan	Action Owner	Current Status	Action Due Date	Status Update
1									
2									
3									
4									
5									

Figure 5-2: Sample Risk Register

- A risk acceptance form/template and completed examples that quantify or qualify likelihood and impact, reference the related non-compliance (if applicable), and record a senior leadership signature with authority to accept risk on behalf of the contractor for the NGCS/ESInet scope.

Motorola Response

Comply.

To protect the integrity of our risk acceptance methodologies and the confidentiality of our existing client environments, Motorola maintains these specific deliverable templates and example artifacts as internal proprietary documentation.

Upon award, Motorola will work with the State to develop mutually agreed upon forms and templates required to support the State of Nebraska deployment and ongoing support of the project.

- Review cadence and triggers, showing at least annual reassessment of all risks and monthly reassessment of critical/high risks; include procedures to re-evaluate on material changes (e.g., carrier migrations, cloud region moves, software upgrades, configuration changes, new interconnections) or emerging threats.

Motorola Response

Comply.

We govern our risk management framework in accordance with NIST SP 800-30 and the NIST Cybersecurity Framework. We treat security as a continuous, operational lifecycle rather than a static checklist, utilizing strict assessment cadences and automated triggers to stay ahead of material changes and emerging threats.

Standard Review Cadence

- **Monthly Reassessment:** Automated vulnerability assessments are executed monthly using industry-leading technical scanning software to immediately identify and neutralize critical or high-risk vulnerabilities.
- **Quarterly Baseline Reviews:** We conduct a mandatory quarterly technical reassessment of all baseline security controls, mapping, and exception handling to ensure strict architectural compliance.
- **Annual Comprehensive Assessment:** A deep-dive, holistic risk assessment and comprehensive vulnerability scan is executed annually to validate the overarching security posture of the entire NG9-1-1 ecosystem.

Triggers for Re-Evaluation (Material Changes)

- **Mandatory ITIL service change request Assessment:** Risk evaluation is tightly integrated into our ITIL Change Management process. The Cybersecurity team actively participates in the Change Advisory Board (CAB); no material change (e.g., carrier migrations, software patches, new interconnections) proceeds without a formal risk assessment.
- **Post-Change Validation Scanning:** Vulnerability scans are explicitly triggered and executed immediately after any major system change that impacts the security perimeter.

- **Emergency Change Triggers:** If quarterly baseline reviews uncover critical control exceptions, an Emergency Change Request is immediately declared, triggering rapid remediation followed by subsequent rescan and revalidation activities.

Triggers for Emerging Threats

- **External Threat Intelligence:** Our 24x7x365 Network Security Operations Center (NSOC) actively leverages external intelligence feeds—including the Public Safety Threat Alliance—to continuously evolve our defenses against zero-day vulnerabilities and newly identified threat actors.
 - **AI-Driven Anomaly Detection:** We utilize advanced SIEM tools and Machine Learning algorithms at the host and firewall levels. Detecting anomalous network traffic patterns instantly triggers deep threat analysis and automated mitigation protocols (such as rate limiting or traffic scrubbing).
-

- A third-party risk approach, including how contractor/subcontractor/carrier/cloud risks are tracked (e.g., supplier registers, attestations), how visibility is maintained when direct control is limited, required compensating controls, and escalation timelines aligned to SLAs/SLOs.

Motorola Response

Comply.

We enforce oversight, continuous monitoring, and strict compensating controls to seamlessly manage risk across all third-party suppliers, carriers, and cloud infrastructure providers.

- **Rigorous Supplier Vetting & Attestations:** Our dedicated Global Supplier organization centrally manages all third-party risks, executing stringent annual or semi-annual performance reviews. All utilized suppliers must pass the same background checks and security clearances as direct Motorola employees. We validate our posture through independent, third-party audits, maintaining ISO 9001:2015 and ISO 27001 certifications alongside SOC 1 Type 2 and SOC 2 Type 2 reports.
- **External Network & Cloud Visibility:** When direct control is limited (e.g., OSP ingress links or third-party clouds), our 24x7x365 NSOC maintains strict visibility using active probes that continuously poll all external connections. Unreachable probes instantly trigger automated incident tickets. Furthermore, our geographically diverse, multi-cloud strategy (e.g., Azure and AWS) allows the NSOC to continuously compare cloud environments to rapidly detect localized vendor degradation.
- **Mandatory Compensating Controls:**
 - **Zero Trust Boundary:** Firewalls enforce strict logical discontinuity between trusted NGCS elements and external networks, operating on a strict "deny-all" posture with explicit allow-listing.
 - **Transport Encryption:** All external connections mandate TLS. If standard TLS is unavailable from a third party, we enforce compensating point-to-point VPN tunnels.
 - **Non-Correlated Risk Routing:** To compensate for unavoidable third-party cloud outages, our architecture automatically acts as a real-time control, instantly steering live 9-1-1 traffic to healthy, distinct regions if one provider experiences a localized failure.

SLA-Driven Escalation Timelines

Third-party incidents and systemic outages are aggressively managed via automated SLA timers within our centralized ITSM platform. Escalations are strictly driven by the percentage of elapsed response time:

- 50% Elapsed: Automated escalation to the Assigned Engineer.
- 75% Elapsed: Automated escalation to the Manager of the Assigned Engineer.
- 100% Elapsed: Automated escalation to the Sr. Manager of Technical Service Delivery.

These automated triggers directly map to our core Incident Severity levels:

- Critical (P1): 15-minute target response (all 50/75/100% escalations trigger within this rapid window). A critical incident bridge is instantly formed and remains continuously active until resolution. Hourly updates are provided. (Note: An automated maximum-severity escalation immediately triggers if any event impacts >50% of the service offering.
 - High (P2): 30-minute target response. Updates are provided every 2 hours.
 - Medium (P3): 4-hour target response. Daily updates provided.
 - Low (P4): Next business day target response.
-

- Non-compliance linkage, showing how unresolved non-compliance (policy gaps, audit findings, penetration test results, vulnerability scans) is converted to corrective action or formal risk acceptance within the same process, with State notification/approval where required.

Motorola Response

Comply.

- We systematically resolve audit findings, security vulnerabilities, and compliance gaps by directly integrating them into our strict, ITIL-based Change and Incident Management processes. This ensures every vulnerability is aggressively converted into a formal corrective action with absolute State oversight.
- **Continuous Identification (NIST SP 800-30):** We execute comprehensive vulnerability scans at initial system turn-up, annually, and following any major architectural change, supplemented by automated monthly assessments. (Note: To protect the 99.999% availability of live 9-1-1 operations, we utilize deep, rate-limited vulnerability scanning instead of disruptive live penetration testing.
- **Quarterly Risk Assessment Reporting (QRAR):** We conduct mandatory quarterly reviews of all baseline security controls. Any identified policy gaps or control exceptions trigger a technical risk reassessment and serve as the primary input for the QRAR.
- **Automated Corrective Actions:** Findings discovered via the QRAR are immediately converted into actionable workflows within our ServiceNow ITSM platform:
 - **Standard Risk:** Spawns a formal service change request to engineer and schedule a fix.
 - **Severe Risk:** Instantly declares an Incident and triggers an Emergency Change Request for immediate remediation.

- **State Notification & Explicit Approval:** The State maintains total control over system modifications. Designated State personnel actively participate in the change review process and must explicitly authorize the service change request before any corrective action is deployed. Real-time progress is fully visible via the CWP.
 - **Mandatory Rescan & Revalidation:** After a corrective action is implemented and the change window closes, we mandate a subsequent rescan and revalidation of the controls to mathematically prove the vulnerability has been successfully eradicated.
 - **State-Identified Non-Compliance:** If the State detects non-compliance during normal operations or testing, they simply open a support ticket. We execute rapid remediation, provide formal written notification of the remedy, and require explicit State acceptance to close the loop.
-

8.1.4 Monthly Project Review and Compliance

The contractor shall meet with the PSC and any of the PSC designated resources at a minimum of monthly throughout the contract period. The frequency of these meetings may be adjusted by the PSC at any time based upon the project lifecycle. Additionally, the agenda of the meeting may be modified based upon any pressing issues that need attention.

The contractor is responsible for providing a report to the State each month that details:

- **Monthly Project review and timeline updates** to document a regular consistent path toward full implementation of the items within the contract
- **Regular Process Audits** to validate adherence to procedures, assess process maturity, and document any corrective actions.
- **Monthly System status and performance** summarizing the performance of the system with details such as utilization, packet success rate, call success rate, traffic path utilization, call transfer updates, database updates, and contract compliance
- **Monthly Service Level Agreement / and Service Level Objective** status vs the KPIs in the SLA.
- **Monthly Risk Management Reports** providing updates to the risk register, risk response (impact and priority) to proactively communicate potential triggers that can cause the system harm.
- **Monthly Change Management Reports** summarizing all changes (planned, emergency, completed, deferred, and failed).
 - **Comprehensive Audit Trails** for all changes, retained for a minimum of three (3) years and available to the State upon request.

The contractors monthly project review process shall:

- Ensure the State is regularly informed of any roadblock or constraint in a proactive manner
- Address issues that arise before they become a barrier

Motorola Response

Comply.

- Regularly assess compliance with applicable **NENA i3** standards.
- Support compliance with **47 CFR Part 9, CJIS Security Policy, HIPAA** (where applicable), and State-level cybersecurity directives.
- Align with **PMI PMBOK** integrated principles.
- Conform to **ITIL v4** practices.
- Ensure traceability of all activities and all provisions of the contract to maintain expectations of the State of Nebraska.

Motorola Response

Comply.

8.2 Continuity and Resilience

8.2.1 Availability

The entire IP path, and call-related services, data transactions, and associated services will be available 99.999% of the time, end to end, with the appropriate caveat for PSAPs that do not have the necessary redundancy to maintain 99.999%. Provisioning services not related to call time, such as provisioning the location database in the LNG by legacy OSPs, will be available 99.9% of the time.

Availability is defined as: $MTBF / (MTBF + MTTR)$

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 99.999% availability for IP path/call services/data transactions end-to-end (with caveat for non-redundant PSAPs).

Motorola Response

Comply.

We provide an uncompromising 99.999% (five-nines) operational service availability SLA for end-to-end call routing and NGCS, ensuring that maximum system downtime never exceeds 5.26 minutes annually.

- **Geo-Redundant Core Architecture:** This five-nines standard is achieved through a multi-cloud design distributed across three geographically diverse regions with zero single points of failure.

- **Dynamic Network Convergence:** We utilize carrier-diverse MPLS circuits and dynamic routing protocols. If a link fails, traffic instantly and automatically fails over to redundant paths without dropping the transaction.
 - **End-to-End Demarcation Scope:** Our SLA accurately measures system performance entirely from the inbound OSP ingress point through to the Valid Destination PSAP demarcation point.
 - **Transparent SLA Exclusions:** To maintain transparency, SLA penalty credits do not apply to issues residing beyond our managed demarcation point. Exclusions include CHE or local LAN failures, insufficient locally ordered bandwidth, customer-provided GIS data inaccuracies, Force Majeure events, and physical facility limitations (e.g., legacy PSAPs lacking diverse building entrances, which are documented and mitigated on a case-by-case basis).
-

- 99.9% for non-call provisioning

Motorola Response

Comply.

Our solution complies with the requirement to maintain uptime standards for administrative, monitoring, and specific connectivity functions. We isolate these services from live traffic to ensure absolute core system stability while guaranteeing reliable access to essential tools.

- **Guaranteed Provisioning & Legacy Support (LNG):** We commit to a 99.9% (three-nines) availability SLA for all non-call-related provisioning services. This explicitly covers critical legacy data integrations, including the routine provisioning of the location database within the LNG by OSPs.
 - **CWP Access:** Our 99.9% SLA extends directly to your administrative tools, guaranteeing consistent, reliable access to the ticketing interface and monitoring dashboard within the CWP for real-time network visibility.
 - **Non-Redundant ESInet Connectivity:** For PSAPs constrained by non-redundant ESInet connectivity (such as legacy facilities lacking diverse building entrances), we explicitly designate a 99.9% availability SLA to ensure maximum possible uptime for these specific edge connections.
 - **Architectural Protection:** By decoupling administrative portals and LNG provisioning functions from our core call-handling databases, we ensure that external updates and monitoring activities never degrade the 99.999% availability of live 9-1-1 call routing.
-

8.2.2 Continuity of Operations Plan (COOP)

The Continuity of Operations plan will include measures to account for common cyber security threats and “sunny day” outage vulnerabilities that could affect the normal operation of the NG911 system and cause an outage.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Measures for cyber threats/"sunny day" outages causing system disruptions.

Motorola Response

Comply.

Motorola's proposed solution includes a comprehensive Business Continuity Strategy and COOP designed to maintain uninterrupted 9-1-1 service during both unexpected "sunny day" outages and malicious cyber events. Our BC preparedness focuses on human-caused, technology-caused, and naturally-caused incidents, aligned with ISO 22301 standards.

Below is a description of the technical measures and operational strategies we employ to prevent and mitigate system disruptions:

Measures for "Sunny Day" Outages and System Disruptions To ensure enhanced survivability and network resiliency during unexpected "sunny day" occurrences or major weather events, our architecture is engineered with no single point of failure and achieves 99.999% operational availability.

- **Active/Active SD-WAN Network:** We utilize High Availability Software-Defined WAN (SD-WAN) edge devices where all primary, secondary, and tertiary circuits are actively processing live traffic at all times. Because all paths are maintained in an active state, there is no delayed "failover" time if a circuit experiences an unexpected drop.
- **Infrastructure Diversity:** Our solution leverages diverse cloud providers, diverse network carriers for ESInet egress, and diverse physical paths to the PSAPs. FEs are distributed across multiple interconnected, redundant, and highly secure Availability Regions so that a single major incident cannot impact more than one region.
- **Facility Resiliency:** Data centers hosting our core services feature redundant power sources (A/B-sided Power Distribution Units), Uninterruptible Power Supply (UPS) systems, and generator backups configured to run for extended periods without intervention, mitigating local power grid failures.
- **PSAP Contingency Routing:** If a PSAP becomes unavailable due to a local outage, our Call Routing Service utilizes customized PRRs and Abandonment Switches. Authorized personnel can instantly activate predetermined emergency scenarios—such as loss of routes, abandonment of a PSAP, or CAD failure—to automatically reroute calls to alternate destinations or backup PSAPs with little to no human intervention.

Measures for Common Cyber Security Threats Cybersecurity is integrated as a core technology rather than an afterthought, utilizing a multi-layered security architecture informed by NENA NG-SEC, NIST, and Department of Defense (DoD) JITC Information Assurance standards.

- **24/7/365 NSOC Monitoring:** Our dedicated NSOC provides continuous, real-time monitoring of all network traffic, system logs, and security alerts. The NSOC uses advanced SIEM tools, machine learning anomaly detection, and IDS/IPS to identify and neutralize threats rapidly.
- **DDoS and TDoS Mitigation:** We address DDoS and TDoS attacks through layered defense mechanisms. The routing service assigns confidence levels to incoming calls to identify malicious traffic patterns. In the event of a TDoS attack, bad-actor traffic is quarantined into specific low-priority call queues, containing the attack and allowing legitimate 9-1-1 traffic to reach telecommunicators unaffected.
- **System Hardening and Network Isolation:** We employ strict network segmentation using firewalls that operate on a "deny-all" principle, permitting only explicitly authorized traffic. Systems are hardened following Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) to significantly reduce the attack surface.

- **Zero-Trust Access Controls:** All physical and virtual access relies on the principle of least privilege, strict RBAC, and MFA via VPNs. No externally exposed attack surfaces or injection points exist within the core network.
-

8.2.3 Disaster Recovery (DR)

The Disaster Recovery Plan will include the procedures for:

- Activation procedures

Motorola Response

Comply.

- Recovery team identification

Motorola Response

Comply.

- Roles and responsibilities

Motorola Response

Comply.

- Recovery strategies and response

Motorola Response

Comply.

- Recovery management procedures

Motorola Response

Comply.

- Recovery cost procedures

Motorola Response

Comply.

- Recovery resources

Motorola Response

Comply.

- Recovery communications

Motorola Response

Comply.

- Stakeholder management

Motorola Response

Comply.

- Subcontractor, Supplier, Partner communication, and coordination

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- DR Plan with activation procedures, team ID/roles/responsibilities, strategies/response, management/cost/resources/communications, stakeholder/subcontractor coordination.

Motorola Response

Comply.

Our BC Strategy aligns with ISO 22301 guidelines, utilizing a rigorous "Plan-Do-Check-Act" methodology to ensure unbreakable 9-1-1 operations during any disruptive event.

Incident Activation & Response

- **Rapid Assessment:** Our Business Continuity Teams (BCT) immediately assesses any reported disruption to determine severity and dictate the appropriate response tier.
- **Targeted Activation:** Minor disruptions trigger targeted facility notifications, while significant events immediately activate a formal Escalation and Notification plan using predefined communication channels.

Continuity Roles & Responsibilities

Table 5-6: Roles and Responsibilities

Team	Primary Function During a Disruptive Event
Emergency Management Organization (EMO)	Directs policy, coordinates overarching disaster response, and manages critical resource allocation.
Business Continuity Teams (BCT)	Manages the direct planning, execution, and success of the continuity plan at the site level.
Designated Response Teams	Deployed by the EMO to rapidly stabilize and restore essential IT, network, and operational processes.

Architectural Resilience & Failover Strategies

- **Geo-Redundant Core:** The system is distributed across multiple cloud providers and diverse availability zones, guaranteeing that the loss of a single physical site will not cause a network failure.
- **Automated PSAP Contingency:** In the event of a local outage, environmental emergency, or facility abandonment, predefined PRRs automatically reroute 9-1-1 calls to designated backup centers or emergency systems.

Management, Communications & Subcontractor Coordination

- **Rapid SLA Communications:** Designated customer stakeholders are notified within 15 to 30 minutes of a critical event, with continuous hourly updates tracked transparently via the CWP.
- **Included Mitigation Costs:** Delivered as a fully managed service, all redundancy, disaster mitigation, and recovery resource costs are built directly into your base service agreements.
- **Single Point of Contact:** Your dedicated Project Manager (PM) assumes total responsibility for all subcontractor coordination, managing regular cadences and expediting issue resolutions behind the scenes to shield your agency from multi-vendor management.

8.3 Operations Centers and Support

8.3.1 Network Operations Center (NOC)

The NOC must operate on a 24x7x365 basis for the duration of the contract. In addition, the NOC will include the capability to perform remote maintenance and restoration of alarms, as necessary.

Motorola Response

Comply.

The NOC will be the single point that performs continuous monitoring, maintenance, and network support services of the NG911 System. The NOC will interface with the help desk and the PSAPs or designated staff. The NOC will be staffed with appropriate technical resources to aid troubleshooting, diagnosis and recovery from issues related to the operation of the NG911 system.

Motorola Response

Comply.

The NOC will perform monitoring of the entire ESInet, all connections and functional components used in the routing of 911 calls. The NOC will be equipped with a Network Management System (NMS) that monitors the performance of the network and infrastructure of the NG911 system.

Motorola Response

Comply.

- The NMS will continuously monitor the performance and availability of all devices.

Motorola Response

Comply.

- The NMS will monitor network performance, including throughput, latency, jitter, packet loss, and other parameters deemed necessary by the State.

Motorola Response

Comply.

- The NMS will monitor the network for network intrusion attempts or security breaches and be capable of issuing security alerts when an event is recognized.

Motorola Response

Comply.

- The NMS will create alarms based on thresholds and parameters and distribute alarm notifications appropriately.

Motorola Response

Comply.

- The NMS will monitor the environment at all data centers or points of presence where critical network components are housed to ensure functionality.

Motorola Response

Comply.

- The NMS will monitor ancillary network components such as power utilization and backup power systems.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24x7x365 NOC with remote maintenance/restoration.

Motorola Response

Comply.

We provide a dedicated 24x7x365 NSOC that is focused on mission-critical public safety and 9-1-1 operations. This NSOC serves as the central point of contact for system monitoring, incident reporting, and both remote maintenance and restoration.

Here is how our NSOC handles remote maintenance and restoration:

- **Remote Troubleshooting and Diagnostics:** The NSOC is staffed around the clock with live, public-safety-trained technicians who can immediately begin remote troubleshooting when an issue is reported or an alarm is generated. NSOC engineers utilize advanced performance monitoring and diagnostic tools to remotely access, evaluate, and diagnose network components, including routers, switches, servers, and workstations.
- **Remote Maintenance and Service Restoration:** To facilitate rapid recovery, customers provide direct, unencumbered remote access to all applicable locations and equipment 24x7x365. This allows NSOC personnel to securely log into the system to perform remote maintenance, execute corrective actions, and restore network or service functionality. By resolving issues remotely, the NSOC significantly reduces MTTR and minimizes the need for time-consuming on-site visits.

- **Escalation to On-Site Support:** While the primary goal is to resolve incidents through remote analysis and corrective actions, the NSOC tracks all incidents based on severity levels. If a critical or high-priority hardware, software, or network issue cannot be fully resolved or restored via remote diagnostics, the NSOC will seamlessly escalate the issue and dispatch local on-site support engineers to restore the system.
-

- Single point for monitoring/maintenance/support.

Motorola Response

Comply.

We provide a streamlined, single-point-of-contact support model that guarantees absolute end-to-end accountability for all NG9-1-1 system monitoring, routine maintenance, and technical resolution.

- **24x7x365 NSOC (Technical SPOC):** Dedicated exclusively to public safety, our Network & Security Operations Center provides a single toll-free number for all issues. The NSOC eliminates vendor confusion by instantly initiating remote diagnostics, troubleshooting, and acting as the sole dispatch point for on-site engineering.
 - **Dedicated Customer Service Manager (Administrative SPOC):** Assigned as your primary lifecycle liaison, this manager oversees continuous SLA compliance, serves as your highest escalation point, and acts as your Change Manager to coordinate all scheduled maintenance and security patching without disrupting operations.
 - **CWP (Digital SPOC):** Our secure "single pane of glass" dashboard integrates directly with our ITSM platform. Authorized users can monitor real-time network health, submit support cases, and track scheduled maintenance events from one centralized location.
 - **Complete Accountability ("One Hand to Shake"):** Because we manage both the NGCS routing and the local Call Handling systems (such as VESTA and CallWorks), we take total responsibility for the entire call flow. We troubleshoot complex network, cybersecurity, or workstation issues comprehensively, completely eliminating multi-vendor finger-pointing.
-

- Interface with help desk/PSAPs.

Motorola Response

Comply.

We provide PSAPs with a comprehensive, multi-tiered suite of support interfaces, seamlessly blending 24x7x365 live technical expertise with transparent, real-time digital dashboards.

- **24x7x365 NSOC Help Desk:** Serving as your central command for incident resolution, the NSOC provides direct access to public-safety-trained technicians. Critical (P1) and High (P2) incidents are immediately escalated via a dedicated toll-free number, while routine inquiries can be efficiently submitted via email or our web portal.
- **CWP:** This secure, "single pane of glass" dashboard delivers real-time situational awareness directly to authorized PSAP personnel. It features live geographical mapping of routing operational states (e.g., active alternate routing or policy exceptions), system health analytics including Voice Quality (MOS) scores, and comprehensive NENA i3 event reporting.

- **Customer Hub (ITSM Ticketing):** Seamlessly integrated into the CWP and powered by our ServiceNow platform, this direct interface empowers users to create routine service requests, communicate directly with assigned engineers, track live ticket progress, and view all upcoming scheduled maintenance or patching events.
 - **Dedicated CSM:** Serving as your primary human interface, this assigned liaison conducts routine operational reviews, manages the ITIL Change Management communication process, and acts as your highest point of escalation for complex support requirements.
-
- Staffed for troubleshooting/recovery.

Motorola Response

Comply.

All troubleshooting and recovery operations are provided by our fully staffed, highly credentialed, public-safety-dedicated experts operating from our 24x7x365 NSOC.

- **Expert-Level Initial Response:** Our NSOC operates far beyond a traditional help desk. Calls are answered by live, certified technicians (holding DoD 8570, Cisco, VM, and Microsoft credentials) who immediately initiate deep remote diagnostics and service restoration, rather than simply logging tickets.
 - **Tiered Engineering Escalation:** If an issue requires advanced intervention, it is rapidly escalated through our highly structured Tier 2, Tier 3, and Tier 4 engineering ranks, who specialize in complex network, software, and hardware troubleshooting.
 - **Guaranteed On-Site Dispatch:** If remote remediation is not possible, the NSOC acts as the central dispatch for local, certified field engineers. For all Critical (P1) and High (P2) incidents, we commit to a maximum 4-hour response time to have a technician physically on-site.
 - **Emergency Response Teams (ERT):** For severe outages impacting the ability to receive 9-1-1 calls, the NSOC immediately activates an ERT. This team establishes a continuous critical incident bridge that remains active and fully staffed until full functionality is restored or a verified workaround is implemented.
 - **DR Operations:** During major business disruptions or catastrophic events, our Emergency Management Organization (EMO) assumes overarching command. The EMO deploys specialized Response Teams expressly dedicated to rapidly recovering essential IT infrastructure, network elements, and business processes.
-

- Monitoring of ESInet/connections/functional components.

Motorola Response

Comply.

We ensure the continuous health, performance, and security of our proposed NG9-1-1 ecosystem through 24x7x365 proactive monitoring executed by our public-safety-dedicated Network Security Operations Center (NSOC).

- **Automated NMS & Active Probes:** Our NMS utilizes active probes to continuously poll all ESInet network devices and NENA i3 functional elements (ESRP, ECRF, LVF, LDB, BCF). This proactive surveillance strictly meets or exceeds NENA-INF-040.2 monitoring best practices.
 - **Performance & Voice Quality (QoS):** We proactively monitor all OSP ingress and ESInet egress connections for bandwidth utilization, latency, jitter, and packet loss. The system continuously tracks MOS, instantly and automatically rerouting traffic around degraded elements to guarantee a pristine voice quality score of 4.0 or better.
 - **Advanced Cybersecurity Monitoring:** The NSOC deploys sophisticated SIEM tools, IDS/IPS deep-packet inspection, and machine-learning anomaly detection. This predictive monitoring instantly identifies abnormal traffic patterns, enabling rapid mitigation of emerging threats such as DDoS and TDoS attacks.
 - **Automated Ticketing & Alerting:** The exact moment a threshold breach is detected, our integrated ServiceNow ITSM platform automatically generates a trouble ticket and triggers user-defined escalation notifications (via email, SMS, or phone) to automatically alert designated agency personnel and dispatch engineers.
 - **Transparent Customer Visibility:** Authorized stakeholders maintain complete, real-time visibility through the secure CWP. This dashboard provides map-based situational awareness, real-time node status, active routing exceptions, and direct access to track live incident tickets and historical SLA reports.
-

- NMS for device performance/availability, network params (throughput/latency/jitter/packet loss), intrusion/breaches with alerts, threshold-based alarms/notifications, data center environment, power utilization/backup.

Motorola Response

Comply.

We provide visibility and protection for our proposed solution NG9-1-1 ecosystem, blending rigorous network performance monitoring with military-grade physical and cybersecurity frameworks.

- **Active NMS & QoS Enforcement:** Our NMS utilizes active probes to continuously monitor all ESInet devices and functional elements. We enforce strict DSCP QoS prioritization to protect mission-critical voice traffic, maintaining stringent budgets for jitter (<20ms), latency (<150ms), and packet loss (<5% end-to-end).
- **Zero-Trust Cybersecurity & SIEM:** Security is baked into our core architecture. The NSOC leverages advanced SIEM tools, IDS/IPS deep-packet inspection, and Machine Learning anomaly detection to proactively neutralize DDoS/TDoS attacks and malicious intrusions.
- **Automated Threshold Alarming:** The instant a performance threshold is breached or an unreachable probe is detected, our ServiceNow ITSM platform automatically generates a ticket. It instantly triggers hierarchical, user-defined alerts (via SMS, email, or voice) to dispatch engineers and notify your designated stakeholders.
- **Uninterruptible Power & Redundancy:** Facilities feature a 2N A+B UPS structure and dual power supplies for all network devices. N+1 diesel generators provide a minimum of 36 hours of continuous backup power at 100% load, backed by aggressive 1-to-4-hour emergency refueling SLAs to ensure absolute continuous operation.

8.3.2 Security Operations Center (SOC)

The proposed solution requires the services of a Security Operations Center (SOC). The SOC (Security Operations Center) may be combined with the NOC and shares the overall requirements. The SOC must provide support for the following items:

- 24×7×365 operation.

Motorola Response

Comply.

- Capability to perform remote maintenance and restoration of security events.

Motorola Response

Comply.

- Single point that performs continuous monitoring, maintenance, and network support services of the NG911 System and identifies security faults.

Motorola Response

Comply.

- Interfaces with the help desk and the PSAPs or designated staff.

Motorola Response

Comply.

- Staffed with appropriate technical resources to aid troubleshooting, diagnosis, and recovery from security issues.

Motorola Response

Comply.

- Perform security monitoring of the entire NG911 system, all connections and functional components used in the routing of 911 calls.

Motorola Response

Comply.

- Security compliance testing, penetration testing, vulnerability testing, etc.

Motorola Response

Comply.

- Collection and monitoring security logs, and assist with incident response

Motorola Response

Comply.

- Operational security administration such as identity & access management, key management, firewall administration, etc.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24x7x365 SOC (possibly combined with NOC) with remote maintenance/restoration of security events.

Motorola Response

Comply.

Motorola operates a combined Network & Security Operations Center (NSOC) that is staffed 24/7/365 by experts dedicated exclusively to mission-critical public safety and 9-1-1 systems. The NSOC continuously monitors the ESInet, network nodes, and system components for performance issues, alarm conditions, and suspicious cyber activity using advanced Security and Event Management tools.

Remote Maintenance and Troubleshooting: When an alarm is triggered or an issue is reported, NSOC technicians do not simply open a ticket; they immediately begin utilizing diagnostic tools to remotely evaluate, troubleshoot, and repair network and system anomalies. To ensure security during these activities, Motorola employs a highly secure remote access solution that requires two-factor authentication, is strictly limited to authorized personnel, and is controlled by the NSOC in real time.

Restoration of Security Events: The NSOC provides active threat mitigation and incident response. If a potential cyber threat is detected, analysts conduct a thorough analysis and implement remote

mitigation strategies, such as blocking malicious traffic via firewalls or applying security patches. In the event of a successful cyberattack or security incident, the NSOC follows a strict incident response plan to:

- Contain the attack to prevent further damage.
- Eradicate the malware or malicious code.
- Restore the affected systems to full functionality remotely

Following restoration, the team conducts a post-incident analysis to identify root causes and implement preventative measures to further secure the system.

- Single point for monitoring/maintenance/support identifying security faults.

Motorola Response

Comply.

Motorola provides a 24/7/365 NSOC that serves as the single point of contact for the entire NG9-1-1 solution, delivering end-to-end accountability for our end-to-end service.

Monitoring & Maintenance: The NSOC proactively monitors all system and network components, generates automated real-time alerts for performance thresholds or hardware faults, manages trouble tickets, and coordinates remote repairs or on-site dispatch.

Identifying Security Faults: Expert personnel continuously monitor the network using advanced SIEM tools to correlate traffic and system logs in real time. If a vulnerability or cyber threat is detected, the NSOC acts as the central command hub to coordinate immediate threat mitigation and incident response.

- Interface with help desk/PSAPs.

Motorola Response

Comply.

Motorola interfaces with PSAPs and handles help desk interactions primarily through its 24/7/365 NSOC, supported by web-based tools and dedicated management personnel. The primary interfaces include:

Telephone (Required for Critical/High Severity): PSAPs can contact the NSOC directly via a toll-free number (such as 1-800-881-4245 or 1-800-MSI-HELP). This connects PSAP personnel with live, trained technical staff who can immediately begin remote troubleshooting rather than simply logging a ticket.

CWPI/ Customer Hub: This secure, web-based dashboard provides direct access to Motorola's IT Service Management system (ServiceNow). Authorized PSAP personnel can use it to submit, track, and update low-priority trouble tickets, request system changes, and view near real-time network status and situational awareness maps.

Email: PSAPs can submit low-priority service inquiries via a dedicated NSOC email address (e.g., VestaNSOC@motorolasolutions.com). Because it is not monitored for an instantaneous response, this channel is strictly for non-urgent requests.

Dedicated CSM: Motorola assigns a dedicated manager to each customer to act as the primary liaison and advocate. This manager oversees day-to-day service needs, reviews service level performance, and serves as a direct escalation point if standard troubleshooting efforts are not meeting the PSAP's expectations.

- Staffed for security troubleshooting/recovery.

Motorola Response

Comply.

Our NSOC is staffed by highly trained technicians who hold Cisco, VM, and Microsoft credentials, empowering them to begin remote troubleshooting immediately. Our NSOC staff also holds DoD 8570 Support Certifications which creates a clear record that the personnel managing your sensitive data have been vetted for competency by an objective third party.

For security events and recovery, these experts utilize advanced SIEM tools to continuously monitor the network, analyze threats, and directly implement mitigation strategies—such as blocking malicious traffic—while following a strict incident response plan to contain cyberattacks, eradicate threats, and fully restore affected systems.

- Security monitoring of system/connections/components.

Motorola Response

Comply.

Motorola's NSOC provides 24/7/365 continuous surveillance of all systems, network connections, and functional components through both active monitoring and passive event collection. To monitor system health and connectivity, the NSOC utilizes network probes deployed throughout the ESInet that actively poll devices; if a component degrades or a connection is lost, it immediately triggers a real-time alarm and automatically generates a trouble ticket.

For dedicated security monitoring, expert analysts continuously evaluate network traffic, system logs, and alerts using advanced SIEM tools to correlate events and rapidly identify potential cyber threats.

This monitoring ecosystem is further reinforced by IDS/IPS, machine learning algorithms that detect unusual network traffic patterns, and routine vulnerability scanning to protect all connections and components across the solution.

8.3.3 Help Desk

A help desk will be included with the NG911 system. The help desk(s) will operate on a 24x7x365 basis and be adequately staffed by resources who are trained and qualified in help desk and customer support services.

Motorola Response

Comply.

The help desk will serve as a single point of contact for all NG911 system and service matters, including without limitation, the NG911 system, all components of the NG911 system, and any additional system service providers delivering services or components for the NG911 ecosystem.

Motorola Response

Comply.

Only a fully staffed help desk will be considered. The help desk must not use an automated attendant or other automated means of answering a call.

Motorola Response

Comply.

The help desk must be accessible via various methods including voice, text, email, and other means as deemed appropriate or as directed by the State.

Motorola Response

Comply.

The help desk will have the ability to communicate directly and immediately with maintenance and support services for the NG911 system and all components of the system, including, without limitation, network troubles. This includes partner providers who are performing or supplying services within the system.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- 24x7x365 staffed help desk trained in support.

Motorola Response

Comply.

Motorola's 24/7/365 NSOC serves as the dedicated help desk and central monitoring hub for mission-critical 9-1-1 systems. It is staffed around the clock by highly skilled technicians specifically trained in NGCS and Call Handling platforms, and who hold advanced credentials such as DoD 8570, Cisco, and Microsoft certifications. Rather than just logging tickets, these experts immediately perform remote troubleshooting and root cause analysis to resolve issues directly. If remote resolution is not possible, the NSOC dispatches on-site support engineers and manages the incident from initial report through to final resolution.

- Single point for all system matters/components/providers.

Motorola Response

Comply.

Motorola's 24/7/365 NSOC functions as the centralized command hub and "one hand to shake" for the entire NG9-1-1 ecosystem, delivering complete end-to-end accountability.

All System Matters and Components: The NSOC provides agencies with a single phone number to call for any incident, actively supporting both the NGCS routing network and the local CHE.

Because Motorola manages the entire call flow from the moment a call enters the network to the moment it is answered at the PSAP, it effectively eliminates vendor "finger-pointing" during troubleshooting and repairs.

All Providers and Suppliers: As the contractor, Motorola assumes full operational oversight and accountability for all third-party suppliers and network carriers used within the solution. The NSOC and Motorola's project teams handle all necessary coordination with these outside entities, including OSPs, ensuring that the customer never has to act as a middleman between different companies to resolve an issue.

Note: No subcontractors or consultants are anticipated for the execution of this project.

- No automated attendant.

Motorola Response

Comply.

Motorola's NSOC has immediate, live support, although an initial automated routing menu is utilized.

When agencies call the 24/7/365 NSOC via the provided toll-free numbers (e.g., 1-800-MSI-HELP or 1-800-881-4245), they are required to follow brief prompts (such as selecting Option 4, 1, 2). This automated menu ensures the call is immediately routed to the correct dedicated 9-1-1 support team

rather than a general queue. Once routed, the call is answered by a live person. Motorola emphasizes that these live NSOC personnel are not just basic call takers; they are highly trained technical experts dedicated exclusively to public safety who can begin troubleshooting your issue immediately.

- Accessible via voice/text/email/etc.

Motorola Response

Comply.

PSAP personnel can access the 24/7/365 NSOC through multiple channels depending on the urgency of the situation. For critical and high-priority incidents, PSAPs should connect via voice by calling the dedicated toll-free number (e.g., 1-800-MSI-HELP or 1-800-881-4245) to immediately engage with live technical experts.

For lower-priority service inquiries and requests, users can reach out via email to a dedicated support address (such as VestaNSOC@motorolasolutions.com) or submit, track, and modify tickets directly through the secure, web-based Customer Hub portal.

While the NSOC utilizes SMS text messaging to push automated outbound notifications and status updates to designated PSAP personnel during outages or critical events, inbound reporting and ticket management are actively driven through phone, email, and the web portal.

- Direct/immediate communications with maintenance/support including network troubles/partners.

Motorola Response

Comply.

Motorola's 24/7/365 NSOC ensures immediate communication by acting as the prime contractor and single point of accountability for all suppliers and subcontractors. If issues cannot be resolved remotely, the NSOC directly dispatches field support engineers and engages next-level management to implement a resolution.

For network troubles, the NSOC proactively monitors connections and coordinates directly with service providers and network carriers to troubleshoot and resolve issues as they occur, ensuring the agency never has to act as a middleman.

8.3.3.1 Trouble Handling and Ticketing Requirements

Trouble handling, and trouble ticket tracking services will be required for the successful operation of the NG911 system and services.

Motorola Response

Comply.

To ensure that all trouble tickets are resolved in a timely manner, The contractor will develop and maintain an escalation guideline document that describes the escalation procedure.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Trouble handling/tracking.

Motorola Response

Comply

Our NSOC utilizes ITSM platform, ServiceNow for trouble handling and ticket tracking. The NSOC manages all incidents from initial report to resolution, handling tickets that are either automatically generated by network monitoring alarms or manually submitted by users via phone, email, or web. Agencies are provided direct, real-time access to the ticketing system through the secure CWP and Customer Hub. This centralized dashboard empowers authorized personnel to easily submit new service requests, track the progression of open trouble tickets, review historical case data, and receive automated status updates via email or SMS as issues are resolved.

- Escalation guideline document/procedure.

Motorola Response

Comply.

Motorola's NSOC manages incident escalations through a defined procedure driven by assigned Severity Levels and automated SLA timers.

As an incident progresses, escalations are automatically triggered based on the percentage of elapsed SLA response time: 50% elapsed time escalates the issue to the Assigned Engineer, 75% escalates it to their Manager, and 100% escalates it to the Senior Manager of Technical Service Delivery.

Critical severity issues are managed aggressively using a critical incident bridge that remains active until a resolution or workaround is implemented.

Additionally, agencies can manually trigger escalations by calling the 24/7 support number to request an on-duty supervisor or by reaching out to successive management contacts, starting with NSOC Management and progressing to Technical Support Operations.

8.3.3.2 Monitoring of Applications and Equipment

Proactive monitoring of all NG911 system components for operation, performance, and fault conditions will be provided.

Motorola Response

Comply.

The contractor will ensure that all alarms including environmental status alarms are received and monitored in a Network Operations Center (NOC).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Proactive monitoring of components for operation/performance/faults.

Motorola Response

Comply.

Our NSOC utilizes advanced network management tools and dedicated probes deployed throughout the ESInet infrastructure. This system conducts continuous surveillance by actively polling and passively collecting events from all networks and functional elements at both the system and application levels.

If performance degrades, a connection is lost, or a component fails, the monitoring tools immediately generate real-time alerts and automatically open a trouble ticket in the IT Service Management system.

This allows NSOC technicians to rapidly evaluate the alarm, initiate remote troubleshooting, and resolve the fault condition to ensure optimal system performance and availability.

- Receipt/monitoring of alarms including environmental in NOC.

Motorola Response

Comply.

Motorola ensures all system and environmental alarms are centrally received and managed through its NSOC.

Automated Alarming: The NSOC continuously polls devices and collects events across all network elements. Any fault or performance degradation immediately triggers a real-time alert and automatically opens a trouble ticket for rapid resolution.

Environmental Monitoring: This continuous 24/7 surveillance extends to facility infrastructure and the "equipment room (environmental)". It ensures that critical environmental controls, such as HVAC and thermal rejection systems, are actively monitored and maintained alongside standard IT components.

8.3.3.3 Root Cause Analysis

The contractor is required to provide a complete Root Cause Analysis (RCA) for any trouble with the system. The RCA process will follow a process like the following:

- Following any critical event or major outage, the State/designated staff must receive a root cause analysis within five (5) business days.

Motorola Response

Comply.

- Immediately after a trouble has been identified the contractor will begin documenting the information as they complete the RCA. This documentation will be made available to the State via a shared online platform that will allow for constant tracking by the State as more information becomes available.

Motorola Response

Comply.

- The RCA format will include dates, times, and discoveries by the contractor as they investigate the trouble.

Motorola Response

Comply.

- Once the investigation has concluded the RCA must be submitted to the State for acceptance and approval that the trouble has been resolved.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- RCA for troubles (within 5 business days for critical/outages).

Motorola Response

Comply.

Motorola agrees to provide an initial root cause analysis for critical (Severity Level 1 and 2) outages within five business days. When a critical outage occurs, Motorola delivers a preliminary Reason for Outage (RFO) report—which includes this initial analysis, an incident timeline, and remediation steps—within five business days of the initial report.

However, a final, in-depth root-cause analysis or Event Analysis Report (EAR) is typically provided later, ranging from 10 to 30 calendar days after the incident's discovery, allowing the necessary time for Motorola to fully recreate and investigate the event.

- Immediate documentation shared online.

Motorola Response

Comply.

To satisfy the need for immediate documentation shared online, Motorola continuously tracks all interactions, troubleshooting actions, and identifies causes within the ServiceNow management system as the event unfolds.

Authorized agency personnel can log into the CWP and Customer Hub at any time to get a near real-time view of active incidents, track the progress of open trouble tickets, and monitor the network's status and ongoing resolution efforts.

- Format with dates/times/discoveries.

Motorola Response

Comply.

Motorola's Root Cause Analysis (RCA)—typically delivered as a Reason for Outage (RFO) or Event Analysis Report (EAR)—follows a structured format to transparently detail an incident. The report specifically includes:

A full timeline of the event: Captures exact dates and times of the outage, troubleshooting interactions, and restoration.

Description and analysis of the event investigation: Documents the discoveries made during the investigation.

Conclusion of the event investigation: Identifies the actual root cause of the outage.

Recommended Actions and Next Steps: Outlines remediation efforts to prevent future occurrences.

Additionally, all interactions, troubleshooting actions, and discovered causes are continuously tracked with precise timestamps in Motorola's ServiceNow management system as the event unfolds.

- Final submission for State approval.

Motorola Response

Comply.

Motorola's responsibility is to ensure the final report is delivered to the State and transparently details the event timeline, the root cause, and the recommended remediation actions to prevent future occurrences.

8.3.4 Customer Support Services

The Respondent must provide a description and/or documentation that supports the requirements in this section, including SLA management (performance/monitoring/delivery/reporting/review); event/incident management; diagnostics/reporting; problem resolution/trouble handling; network fault monitoring; request fulfillment; access management; remote diagnostics; environmental requirements; capacity/change/configuration/transition management; training; commercial availability; all tied to SLOs for SLA measurement.

Motorola Response

Comply.

The contractor is required to provide monthly updates to the PSC regarding the performance of the system in the form of a Monthly Performance Review which is used to measure adherence to the contract elements, the performance measures, and Key Performance Indicators (KPIs). The KPIs are directly tied to the SLA.

Motorola Response

Comply.

Motorola complies with the requirement to provide monthly performance updates tied to SLAs and KPIs. Through its automated service management systems, Motorola generates comprehensive monthly SLA compliance reports that detail key performance metrics, including system availability, voice quality, network performance, and incident resolution times. To ensure strict adherence to contract elements, a dedicated Operations or CSM is assigned to conduct these scheduled monthly performance reviews with the customer, analyzing SLA achievements, reviewing any service failures or tickets, and discussing continuous service improvements.

Anticipated support services include:

- Service Level Agreement (SLA) management
 - Performance measurement and monitoring
 - Guaranteed delivery
 - SLA reporting and review

Motorola Response

Comply.

Motorola comprehensively fulfills these anticipated support services through its NSOC and dedicated Customer Service/Operations Managers:

SLA management: A dedicated CSM oversees all contracted services and works directly with the agency to ensure service levels are strictly maintained. Motorola's ITSM platform automatically tracks SLA timers and triggers immediate escalation procedures if an incident breaches specific elapsed-time thresholds.

Performance measurement and monitoring: The NSOC conducts continuous 24/7/365 active monitoring and passive event collection across all network and functional elements. Authorized agency personnel are granted secure access to the CWP, which features an executive dashboard displaying near real-time network status, bandwidth utilization, and performance health metrics.

Guaranteed delivery: The solution is architected with multiple layers of geo-diversity and redundancy to guarantee 99.999% operational system availability. This is backed by a specific "Call Delivery" SLA, which guarantees that all calls entering the system are successfully delivered to a valid destination.

SLA reporting and review: Automated, comprehensive SLA compliance reports are generated monthly, detailing key metrics such as service availability, voice quality, network performance, and trouble ticket resolution times.

The assigned CSM conducts scheduled monthly and quarterly reviews with the customer to analyze SLA achievements, review any service failures, and discuss continuous service improvements.

-
- Event management

Motorola Response

Comply.

-
- Incident management

Motorola Response

Comply.

-
- Diagnostics and reporting

Motorola Response

Comply.

- Problem resolution/trouble handling

Motorola Response

Comply.

- Network fault monitoring

Motorola Response

Comply.

- Request fulfillment

Motorola Response

Comply.

- Access management

Motorola Response

Comply.

- Remote diagnostics

Motorola Response

Comply.

- Environmental requirements

Motorola Response

- Capacity management

Motorola Response

Comply.

- Change management

Motorola Response

Comply.

- Configuration management

Motorola Response

Comply.

- Transition management

Motorola Response

Comply.

- Training arrangements

Motorola Response

Comply.

- Commercial availability

Motorola Response

Comply.

Each of the items listed above are tied to Service Level Objectives (SLO) that the State measures against the Service Level Agreement (SLA).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- SLA management (performance/monitoring/delivery/reporting/review) on a monthly basis to the PSC.

Motorola Response

Comply.

Our dedicated CSM is responsible for monitoring SLA performance and conducting reviews with the customer. SLA adherence is tracked automatically, and automated monthly statistical reports are delivered to the customer, detailing network performance, system availability, component availability, voice quality, and call delivery metrics. Authorized personnel can also run on-demand SLA reports and monitor performance in real-time via the secure CWP.

- Event/incident management.

Motorola Response

Comply.

Our NSOC manages all incidents, from user-reported issues to automatically generated system alerts. Incidents are managed through an IT Information Library (ITIL)-based framework using the ServiceNow ITSM toolset. Incidents are classified into four severity priority levels (Critical, High, Medium, Low), which dictate the target response times, communication update intervals, and escalation paths.

- Diagnostics/reporting.

Motorola Response

Comply.

Our NSOC utilizes advanced performance monitoring and diagnostic tools to monitor routers, switches, and servers remotely. The solution includes comprehensive reporting platforms, such as the i3 Event Logger and MIS reporting, which offer standard, management, and ad-hoc reports. In the event of a significant service outage, We provide a preliminary Event Analysis Report (EAR) or Reason for Outage (RFO) report, followed by a final root-cause analysis report that details the timeline, diagnostic findings, and preventative steps.

- Problem resolution/trouble handling.

Motorola Response

Comply.

Upon notification of an incident, the NSOC performs remote analysis to identify a corrective action plan and resolve the issue. If the NSOC cannot resolve the service issue remotely, the case is escalated to specialized technical support engineers or local field technicians are dispatched to ensure timely problem resolution. Problem management processes include long-term retention of trouble resolutions to enable continuous improvement and reduce the frequency of future incidents.

- Network fault monitoring.

Motorola Response

Comply.

All network, computing, and software elements are continuously monitored by the NMS within the NSOC. The monitoring system utilizes active probes deployed throughout the ESInet; if a probe becomes unreachable or a specific performance threshold is breached, the system automatically generates an actionable alarm and opens a trouble ticket.

- Request fulfillment.

Motorola Response

Comply.

The Customer Hub serves as the user interface into the incident and request management structure. Through this portal, users can create service requests, submit service change requests, ask general informational questions, and track the real-time status and progression of their requests.

- Access management.

Motorola Response

Comply.

Access is secured physically and logically. Physical access to data centers is restricted using multiple layers of electronic safeguards, including biometric controls, proximity cards, locking cabinets, and two-factor authentication. Remote access to portals and user interfaces employs RBAC and requires MFA.

- Remote diagnostics.

Motorola Response

Comply.

The system is engineered to allow NSOC personnel to remotely access, troubleshoot, diagnose, and repair network and system faults.

- Environmental requirements.

Motorola Response

Comply.

The core NGCS elements are deployed in a highly reliable, geographically diverse multi-cloud environment. These facilities are rated at a minimum of Tier 3 for thermal rejection and Tier 4 for power, featuring redundant Computer Room Air Conditioning (CRAC) and UPS with generator backups.

- Capacity/change/configuration/transition management; training.

Motorola Response

Comply.

- **Capacity:** The system is scalable and engineered to handle 125% of busy hour call traffic, with the ability to support voice and data bandwidth growth of 50% without requiring hardware replacements.
 - **Change & Configuration Management:** Managed by the CSM via an ITIL-based process. All system updates, patches, and configurations require a formal service change request, the development of an implementation plan, a rollback plan, and formal approvals.
 - **Transition Management:** Phased Transition and Cutover Plans are developed to ensure the non-service-affecting migration of OSPs and PSAPs from legacy systems to the new NGCS environment.
 - **Training:** A comprehensive Training Plan provides customized instruction for system administrators and supervisors using a combination of virtual, web-based, and instructor-led training.
-

- Commercial availability.

Motorola Response

Comply.

Our NG9-1-1 solution is a commercially available, market-ready platform delivered "as a service". It is currently deployed and fully operational in major statewide and regional networks, including the State of Utah, State of New Mexico, and Greater Harris County, Texas.

- All tied to SLOs for SLA measurement

Motorola Response

Comply.

Every aspect of our service is governed by strict Service Level Objectives (SLOs) and SLAs. Target response times are explicitly tied to the priority level of the incident (e.g., a 15-minute response target for P1 outages). System SLAs measure metrics such as a 99.999% operational availability for call routing and Voice Quality standards (PMOS above 3.5), with automated timers triggering escalations.

8.4 Monitoring and Event Management

8.4.1 Alarm Categories

Alarms by event types depending on the criticality of the event (i.e., critical, major, etc.) will be provided. Dynamic configuration of notification thresholds will be utilized to allow new alarm categories to be defined, as necessary.

Motorola Response

Comply.

The system will have automatic notification of the NOC when alarm conditions are detected. Different notification and escalation procedures may apply depending on the alarm category.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Alarms by criticality (critical/major/etc.).

Motorola Response

Comply.

The monitoring system utilizes active probes to continuously poll all network devices and functional elements. When alarms are received, they are correlated by the NSOC monitoring solution and presented as incidents classified into distinct severity levels based on their impact. The system strictly categorizes these alarms and resulting tickets into four priority tiers:

- **Critical (Priority 1):** Significant and/or severe degradation of service functionality that impacts inbound call or associated location processing, with no workaround available.
 - **High (Priority 2):** Significant degradation of service functionality that impacts inbound call or associated location processing where a workaround may be available.
 - **Medium (Priority 3):** A minor degradation of service functionality or capacity of inbound call or associated location processing.
 - **Low (Priority 4):** A degradation of system functionality that does not impact inbound call or associated location processing.
-

- Dynamic notification thresholds for new categories; automatic NOC notification.

Motorola Response

Comply.

Our solution features automated alarming and ticketing that immediately alerts the NSOC without requiring human intervention. If a network probe becomes unreachable, a trouble ticket is automatically generated in the Service Management System.

Furthermore, the ITSM toolset supports auto-generated notifications based on multiple user-defined thresholds. These dynamic thresholds can be configured to trigger notifications based on the severity of an issue, a specific type of activity (like a change authorization request), or whenever a specific performance threshold is breached on a network link or component. Additionally, the system features automated safety nets; for example, an automated escalation and notification sequence will commence immediately if an event impacts more than 50% of the service offering or if an alarm is not acknowledged within the defined timeframes.

- Varying notification/escalation per category.

Motorola Response

Comply.

Notification intervals and escalation paths are dynamically dictated by the specific severity category of the alarm.

- **Communication Intervals:** A Critical (P1) incident mandates a response within 15 minutes and hourly notification updates to stakeholders. A High (P2) incident mandates a response within 30 minutes and updates every 2 hours. Medium and Low issues require daily or as-needed updates, respectively.
 - **Automated Escalation Timers:** The Service Management System automatically starts SLA timers the moment an incident is detected. Escalations are automatically triggered based on the percentage of the SLA response time that has elapsed.
 - At 50% of elapsed time, the issue escalates to the Assigned Engineer.
 - At 75% of elapsed time, it escalates to the Manager of the Assigned Engineer.
 - At 100% of elapsed time, it escalates to the Sr. Manager of Technical Service Delivery.
 - **Incident Handling Variations:** For Critical severity issues, the escalation process is managed much more aggressively. The NSOC initiates an Emergency Response Team (ERT) and establishes a critical incident bridge that is not disbanded until a resolution or temporary workaround is implemented.
-

8.5 Change, Maintenance, and Release Management

8.5.1 Change Management Requirements

The Contractor shall ensure that all changes – planned or unplanned – are managed through a structured, documented, and auditable process that maintains service stability, security, and interoperability. The process shall conform to the principles of the **Project Management Institute (PMI)** and the **ITIL v4 Service Management Framework**.

Objectives

The objectives of the Contractor's Change Management process shall be to:

- Maintain a stable and secure NG9-1-1 operational environment.
- Minimize the impact of changes on system availability, reliability, and public safety operations.
- Provide transparency and accountability for all system modifications.
- Ensure that all stakeholders are informed, consulted, and prepared for any change that affects service delivery.
- Incorporate continuous improvement through post-implementation review and process enhancement.

The Change Management process shall apply to all infrastructure, applications, systems, and interfaces under Contractor operational control, including but not limited to:

- **ESInet Infrastructure:** routers, firewalls, switches, circuits, transport paths, and interconnections.
- **NGCS Components:** ESRP, ECRF/LVF, PRF, BCF, LIS, logging, and policy routing elements.
- **Call Handling Systems:** software, hardware, operating systems, and integrations with CAD, logging, and recording systems.
- **Security Systems:** encryption, certificates, firewalls, intrusion detection/prevention, and access controls.
- **Support and Management Tools:** monitoring platforms, ticketing systems, and network management applications.

Change Classification

The Contractor shall classify all changes into the following categories:

- **Standard Change:** Pre-approved, low-risk, repeatable changes executed according to pre-established procedures (e.g., routine software patching).
- **Normal Change:** Planned changes that require full evaluation, testing, review, approval, and scheduling.
- **Emergency Change:** Unplanned changes necessary to restore service, mitigate critical vulnerabilities, or prevent imminent service degradation.

Each classification shall have documented criteria, approval authorities, and implementation procedures.

Process Requirements

The Contractor shall implement a formal Change Management process that includes the following elements:

- **Change Management Plan:** A documented process outlining governance, roles, responsibilities, and workflows aligned with PMI and ITIL best practices.
- **Change Advisory Board (CAB):** A standing review body, including State representation, responsible for evaluating and approving all Normal and Major Changes.
- **Change Request System:** A centralized, auditable tool for logging, tracking, and managing all changes from request through closure.
- **Risk and Impact Assessment:** An analysis of each proposed change to evaluate its impact on system performance, service continuity, interoperability, and cybersecurity.
- **Rollback and Contingency Plans:** Documented procedures for reverting or recovering from unsuccessful change implementations.
- **Change Scheduling and Coordination:** Change windows coordinated with the State and PSAPs to minimize service disruptions.
- **Notification Requirements:** Written notice to affected stakeholders no less than ten (10) business days prior to implementation of any planned change, unless otherwise authorized.
- **Post-Implementation Review (PIR):** A formal evaluation of significant or failed changes to identify root causes, corrective actions, and process improvements.

Emergency and Security Changes

- The Contractor shall maintain procedures for the execution of emergency changes required to restore service or address urgent security vulnerabilities
- All emergency changes shall be documented and submitted for retrospective review by the CAB within five (5) business days.
- Security-related changes, including software updates, certificate renewals, or configuration modifications, shall comply with PMI and ITIL Change Enablement best practices.
- Security changes shall be tested in a controlled environment prior to production deployment whenever feasible.
- The Contractor shall notify the State of any emergency or security change within twenty-four (24) hours of implementation.

Integration with Other Service Management Processes

The Contractor shall integrate Change Management with the following processes:

- **Configuration Management:** Each change shall be linked to affected Configuration Items (CIs) within the Configuration Management Database (CMDB).
- **Incident Management:** Changes shall be correlated with incident and problem records to support root cause analysis and continuous improvement.
- **Release and Deployment Management:** The Contractor shall coordinate releases to ensure version control and documentation integrity across environments.

Motorola Response

Comply.

To ensure every requirement of section 8.5.1 is addressed, the following response details how our **Service** model fulfills each specific mandate through the Motorola NSOC and our ITIL v4 framework.

The Motorola service utilizes a structured, auditable change management process that ensures service stability and security. By delivering this as a managed Service, we handle the technical execution while providing the State with full governance and transparency.

Objectives

Our process is designed to achieve the following:

- **Stability:** Maintain a secure and stable NG9-1-1 environment through rigorous testing.
- **Minimal Impact:** Schedule updates to minimize effects on system availability and public safety operations.
- **Transparency:** Provide clear accountability for every modification via our centralized portal.
- **Stakeholder Readiness:** Ensure the State and PSAPs are informed and prepared for upcoming changes.
- **Continuous Improvement:** Utilize Post-Implementation Reviews (PIR) to enhance future workflows.

Scope of Application

This process applies to all components under Motorola's operational control, including the ESInet Infrastructure (routers, firewalls, circuits), NGCS Components (ESRP, ECRF/LVF, BCF, LIS), Call Handling Integrations, Security Systems (certificates, encryption), and Support Tools (monitoring and ticketing platforms).

Change Classification

All service modifications are categorized with specific approval authorities and implementation procedures:

- **Standard Change:** Pre-approved, low-risk, and repeatable (e.g., routine software patching).
- **Normal Change:** Planned changes requiring full evaluation, testing, review by the CAB, and scheduling.
- **Emergency Change:** Immediate actions required to restore service or mitigate critical security vulnerabilities.

Process Requirements

The Service incorporates a formal Change Management Plan aligned with PMI and ITIL v4:

- **Change Advisory Board (CAB):** A standing body with State representation to review and approve Normal and Major changes.
- **Change Request System:** A centralized, auditable tool used for logging and tracking changes from request to closure.
- **Risk and Impact Assessment:** Mandatory analysis for every change regarding performance, continuity, and cybersecurity.
- **Rollback and Contingency Plans:** Documented procedures for immediate recovery if a change is unsuccessful.
- **Scheduling and Notification:** Maintenance windows are coordinated during off-peak hours. We provide at least **10 business days** advance notice for planned changes.

Emergency and Security Changes

Motorola maintains specialized procedures for urgent service or security needs:

- **Rapid Execution:** Emergency changes are performed to restore service or address vulnerabilities, with State notification within **24 hours**.
- **Retrospective Review:** All emergency actions are submitted to the CAB for review within **5 business days**.
- **Security Integrity:** Security updates are tested in controlled environments prior to deployment to ensure interoperability and stability.

Integration with Other Service Management Processes

Our Change Management process is natively integrated into our broader service ecosystem:

- **Configuration Management:** Every change is linked to Configuration Items in our CMDB, providing an accurate "as-built" view.
 - **Incident Management:** Changes are correlated with incident and problem records to facilitate Root Cause Analysis (RCA).
 - **Release and Deployment:** We coordinate releases to ensure version control and documentation integrity across all environments.
-

8.5.1.1 Security Considerations in Change Management

In conjunction with the change management processes defined in §E-9.5.2 (Scheduled Maintenance Process) and §E-9.5.3 (Software Update and Improvements) of this document, the contractor must evaluate the security impact and operational risk for all changes to NGCS elements and the ESInet – including equipment, software, and configurations. Every change requires policy-compliant review and approval, a documented security review, and complete records. If timing precludes standard pre-approval (Unplanned/Emergency [time-critical issues with expedited workflows] issues), all required reviews and documentation must be completed immediately after implementation. The contractor should utilize segregation of duties, maintain configuration baselines, and coordinate maintenance windows to protect call delivery, routing, location accuracy, latency, and availability.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Evidence that all changes are reviewed and approved per policy with a documented security review (threat/impact, affected NGCS/ESInet elements and services, potential customer impact, required controls and monitoring).

Motorola Response

Comply.

We provide auditable evidence for every system modification through our ServiceNow ITSM platform. The formal service change request record serves as the definitive proof that all changes undergo rigorous, policy-compliant security reviews and stakeholder approvals prior to implementation.

- **Mandatory Security Reviews & Approvals (service change request process):** Every planned change requires a formal service change request. The Cybersecurity department and the Change Advisory Board (CAB) actively review each service change request to evaluate operational risk and security impact. This documented review explicitly captures the identified threats, affected NGCS/ESInet services, potential customer impact, and the necessary compensating controls and monitoring required during the deployment window. No change proceeds without documented approval from all designated stakeholders.
 - **Segregation of Duties & Configuration Baselines:** We enforce strict segregation of duties across our deployment pipeline—ensuring that personnel who develop or test changes are explicitly restricted from authorizing or deploying them into the live production environment. All changes are validated against established configuration baselines to prevent unauthorized architectural drift.
 - **Coordinated Maintenance Windows:** To safeguard the 99.999% Operational Availability SLA, all standard changes are strictly coordinated and executed during predefined, low-traffic maintenance windows, fully transparent to the agency via the CWP.
-

- An Unplanned/Emergency change process that documents expedited approvals and requires retroactive completion of all "SHALL" requirements and documentation identified in NENA-STA-040.2 §4.4 (Change Management) within a defined timeframe.

Motorola Response

Comply.

We recognize that critical, service-impacting events require immediate mitigation. Our Emergency Change Request process provides an expedited workflow to restore life-safety operations without sacrificing compliance.

- **Expedited Approvals:** In the event of an unplanned, time-critical issue (such as a zero-day vulnerability or active network outage), the CAB convenes an emergency bridge to grant immediate, expedited verbal or digital approval to deploy the necessary fix.
 - **Retroactive NENA-STA-040.2 Compliance:** If timing precludes the standard pre-approval documentation, our policy mandates that all standard risk assessments, security reviews, and complete records be finalized retroactively. We strictly require the completion of all "SHALL" requirements identified in NENA-STA-040.2 §4.4 (Change Management) within a defined 24-to-48-hour timeframe immediately following the emergency implementation, ensuring the system's audit trail remains unbroken.
-

8.5.2 Scheduled Maintenance Process

A scheduled maintenance process document will be developed and maintained. The process must include a methodology for coordinating and scheduling preventative maintenance activities and how those events are executed as may be necessary during the operation of the NG911 system.

Motorola Response

Comply.

During scheduled maintenance activities the ESInet and NG911 system must maintain 99.999% availability. There must not be a substantial degradation or disruption caused by the maintenance activity. However, individual components may be taken down for maintenance if an alternate route or redundant system is used to maintain the 99.999% threshold.

Motorola Response

Comply.

If a partial or total outage occurs within hours of a maintenance activity, Contractor shall issue a report within 30 days to the State detailing:

- What occurred during the outage, including system elements that were impacted?

Motorola Response

Comply.

- Whether the outage was caused by, or influenced by, the maintenance activity

Motorola Response

Comply.

- What corrective actions, specifically corrective actions to the change control process, will be implemented to avoid recurrence, not just to the specific problem but to similar problems

Motorola Response

Comply.

Following any scheduled maintenance, a maintenance report must be prepared and sent to the State within 24 hours, detailing:

- What are the results of the scheduled maintenance?

Motorola Response

Comply.

-
- What was done during the scheduled maintenance

Motorola Response

Comply.

- How will such scheduled maintenance impact the services in operation?

Motorola Response

Comply.

Following any emergency maintenance, an emergency maintenance report must be prepared and sent to the State within 24 hours, detailing:

- What caused the emergency maintenance?

Motorola Response

Comply.

- What was done during the emergency maintenance

Motorola Response

Comply.

- How will such emergency maintenance be avoided in the future?

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Developed/maintained process document for coordinating/scheduling preventative maintenance.
- No degradation/disruption during activities.
- Allowance for individual component downtime with alternates/redundancy.

Motorola Response

Comply.

Motorola utilizes a proven, standardized, IT Information Library (ITIL)-based Change Management methodology to seamlessly schedule and perform all preventative maintenance events. To ensure transparency and minimize disruption, all scheduled maintenance activities are formally entered, logged, and tracked as change requests within our ITSM tool, ServiceNow.

Maintenance Approach

A core principle of our maintenance strategy is that there shall be no system downtime or service degradation during routine maintenance activities. Our service is engineered with a highly available, redundant architecture that eliminates single points of failure. This allows for safe, individual component downtime during scheduled maintenance. When a specific hardware or software element requires servicing, the system seamlessly leverages alternate or redundant components to maintain full-capacity call processing and uninterrupted operational continuity.

Documented Coordination Process

Our documented process for coordinating preventative maintenance follows these key steps:

- **Pre-Notification and Summary:** Before any work begins, we generate an overview summary of the proposed maintenance event detailing exactly what actions will be taken and the operational reasons why. This pre-notification summary is provided directly to the Motorola CSM.
- **Customer Coordination:** The CSM acts as the primary point of contact to pass this notification on to the customer. They ensure the customer is notified of all planned work that may affect functionality within a mutually agreed-upon timeframe prior to the event, unless an emergency change must be implemented.
- **Completion Notification:** Once the preventative maintenance is successfully executed, we close the communication loop by sending a formal "completed" notification to the customer.

Emergency Maintenance & Root Cause Analysis (RCA) Procedures

While our standard methodology prioritizes scheduled preventative maintenance, our process is built to rapidly accommodate scenarios where an emergency change must be implemented. In these instances, we provide a rapid overview summary of the emergency maintenance events, transparently outlining what we are going to do and why.

Following the resolution of a priority 1 incident or emergency maintenance event, we utilize a formal Root Cause Analysis (RCA) to investigate, track, and communicate findings back to the customer. The RCA documentation process includes:

- **In-Depth Reporting:** We generate a Reason for Outage (RFO) or RCA report that provides a full timeline and description of the event.
- **Investigation & Analysis:** The report details the complete analysis and conclusions of the event investigation.
- **Actionable Next Steps:** We provide recommended actions and next steps to mitigate future risks. Ultimately, the RCA formally documents how similar incidents or the need for emergency maintenance can be avoided in the future.

8.5.3 Software Development Process

The Contractor and all Subcontractors shall use a documented, modern software development lifecycle (SDLC) that produces high-quality code with minimal delay. At a minimum, the SDLC shall include secure coding standards, peer/code reviews, automated testing, version control, and controlled release management (CI/CD or equivalent).

Motorola Response

Comply.

For all software components directly in the NG911 call path, the Contractor and all Subcontractors shall have a process to evaluate, release, and deploy critical security patches within 72 hours of the patch's public availability. This process shall be rehearsed on a regular cadence, and rehearsal results shall be shared with the State.

Motorola Response

Comply.

When a trouble ticket or outage results in a software bug, a discrepancy report, or a required system change to prevent recurrence, the Contractor shall maintain an online, State-accessible log showing each item, severity, affected components, current status, workaround (if any), and the target fix version and release date. This log shall also include items required to bring the system into conformance with standards such as NENA-STA-010.3(including the Discrepancy Reporting function).

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Modern processes for high-quality code with minimal delay.

Motorola Response

Comply.

Our documented SDLC process guarantees high-quality code delivery with minimal delay. All software releases mandate strict secure coding standards, mandatory peer/code reviews, comprehensive automated testing, and strict version control, all orchestrated through an advanced Continuous Integration/Continuous Deployment (CI/CD) pipeline.

- 72-hour release/install for critical security patches with rehearsal/results shared.

Motorola Response

Comply.

Our goal is to release and install critical security patches within 72 hours of their public availability. This expedited timeframe is strictly contingent upon the successful evaluation and rigorous testing of the patch within our sandbox environments to guarantee it will not degrade system performance.

- Log of bugs/changes/estimated fixes available online.

Motorola Response

Comply.

If a software bug or system fault is detected, it is immediately reported and tracked using our ITSM tool, ServiceNow, alongside JIRA for issue tracking. State and agency personnel are provided access to the CWP and Customer Hub, which act as a direct window into the ServiceNow ticketing system. Through this online dashboard, authorized users can monitor the real-time progress of open trouble tickets, issue resolution, and view scheduled events such as upcoming software changes and security patches.

- Updates for standards conformance.

Motorola Response

Comply.

As industry standards evolve, we continuously upgrade our service to maintain compliance with the latest requirements. The architecture is designed to support and incorporate new and applicable standards within 18 months after formal ratification by organizations like NENA. Importantly, as these updates are made to achieve compliance, they are engineered so they will not abandon existing services or feature functionality.

8.5.4 Software Updates and Improvements

Updates, bug fixes, and patches must be classified by the contractor as normal or emergency. When any normal hardware or software changes are made to a site, there will be a minimum of 30 days before any hardware or software changes can be made to any other site. Where more than one instance of a function or service is provided on a site, only one instance can be changed at a time. Where there are both multiple sites and redundant instances per site, one instance may be changed at the first site, at least 30 days must elapse, one instance on another site can be made, at least two weeks must elapse, another instance can be updated, after which at least one week must elapse before the next change.

Motorola Response

Comply.

Emergency bug fixes/patches are not required to meet these minimum times. However, if the contractor determines that an emergency bug fix/patch is necessary, it will transmit a report to the State within 48 hours of such a determination, detailing the problem, the necessary fix, and a valid reason the fix could not be completed in regular software update or bug fix processes.

Motorola Response

Comply.

A prescheduled maintenance window will be negotiated between the contractor and the State. All normal maintenance will take place within that window. Extra-ordinary maintenance processes that require additional time may be scheduled with a minimum of 30 days' notice.

Motorola Response

Comply.

Emergency maintenance can be scheduled with no prior notice, but the State must be notified immediately that such an emergency maintenance is needed, what the estimated duration is and why the emergency maintenance is necessary.

Motorola Response

Comply.

The Respondent must provide a detailed methodology for managing all system updates, including software patches, security updates, configuration changes, and data updates (e.g., GIS data). The process must be structured to minimize service disruption, ensure system integrity, and maintain security. The update process must include procedures for testing, scheduling, deployment, and verification of all changes in the production environment.

Motorola Response

Comply.

A formal process for releasing software updates, bug fixes and improvements, and any changes to the process will be communicated to the State within 30 days of the change being put into practice.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Formal process for updates/fixes/improvements with 30-day notice of changes.

Motorola Response

Comply.

We manage all changes through a formal service change request process tracked within its ITSM toolset.

Any proposed changes to requirements, network services, application patches, or software updates are evaluated by a Change Advisory Board (CAB), which includes actively participating Cybersecurity personnel.

We collaborate with the State to develop a customized Customer Support Plan (CSP). Through this governance and the formal service change request approval process, Motorola can easily accommodate the requirement to provide 30 days advance notice for normal changes and communicate any modifications to the update process itself within 30 days of implementation.

- Classification as normal/emergency.

Motorola Response

Comply.

Motorola's ITIL change profile guidelines mandate that all updates, bug fixes, and patches be explicitly classified. Changes are evaluated based on their identification, prioritization, impact, risk, and type, and are strictly categorized as either normal/scheduled maintenance or emergency changes.

Critical security threats or severe vulnerabilities are classified as Emergency Change Requests so they can be expedited through testing and deployed as safely and quickly as possible.

- Minimum 30-day spacing for normal changes across sites/instances.

Motorola Response

Comply.

Before a service change request is officially scheduled, it must include a detailed implementation plan, a rollback (back-out) plan, and formal approval from the State's designated personnel. Therefore, no normal changes are promoted to the production environment without the State's direct authorization.

Because the State dictates the approval and scheduling of the service change request, our CSM will enforce the required staggered implementation sequence (30 days between different sites/instances) during the scheduling phase to guarantee compliance.

- No minimum times for emergency but 48-hour report to State.

Motorola Response

Comply.

Emergency bug fixes and critical security patches bypass standard minimum spacing intervals to ensure the service is immediately protected.

If an emergency fix is deemed necessary, Motorola's NSOC utilizes its incident management and Root Cause Analysis (RCA) reporting structures. The NSOC can transmit a report to the State within the required 48-hour window detailing the exact problem, the implemented fix, and the justification for bypassing the normal update process.

- Negotiated maintenance window.

Motorola Response

Comply.

We will work directly with the State and affected PSAPs to negotiate prescheduled maintenance windows.

The CSM (acting as the Change Manager) ensures that all normal, non-emergency maintenance is strictly scheduled and executed within the mutually agreed-upon maintenance window to prevent disruption to day-to-day 9-1-1 operations.

- Extra-ordinary with 30-day notice.

Motorola Response

Comply.

If an update or maintenance process impacts the 30-day notice timeline, it is flagged during the service change request assessment phase. The CSM will coordinate with the State to schedule this extra-ordinary maintenance event.

- Immediate notification for emergency with duration/reason.

Motorola Response

Comply.

Our NSOC provides immediate notification for any emergency maintenance or critical, service-impacting events. Notifications are dispatched within 15 minutes of the event's discovery via phone call, email, or SMS text message.

The initial notification conveys all available information, including the nature of the emergency, the reason the maintenance is necessary, and the estimated duration for repairs, followed by continuous hourly updates until the issue is resolved.

8.6 Spares and Inventory

8.6.1 Spares

Respondents must describe their spares program, including stocking levels, storage locations, and the time required for an on-site field technician to obtain a spare. If the State has any role in spare stocking or access, explain that role.

Motorola Response

Comply.

A sufficient supply of spare parts shall be maintained at locations that enable immediate restoration of service. This requirement is tied to the Mean Time to Repair (MTTR) specified in SE-9 of this document. Where there are multiple connections, the Contractor shall provide multiple spare units staged in multiple locations.

Motorola Response

Comply.

Within the proposal response, explain how sparing strategies maintain both Mean Time Between Failures (MTBF) and MTTR at levels necessary to achieve 99.999% availability.

Motorola Response

Comply.

If malfunctions or failures recur, the State may require the Contractor to increase spare inventory to ensure adequate parts are available to address the repeated issue.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- Describe the spares program, including stocking levels, locations, and technician access time

Motorola Response

Comply.

Locations & Stocking Levels: To enable immediate restoration of service and meet MTTR objectives, spares are geographically staged at our parts depots rather than centralized in a single national warehouse. The primary on-site equipment required for the routing service consists of High Availability (HA) SD-WAN Edge Devices. Multiple spare units are staged locally to support the volume of deployed connections.

Technician Access Time (MTTR): The Motorola NSOC actively monitors all devices. If an alarm indicates an Edge Device has a service event, the NSOC generates a trouble ticket and dispatches a local field technician. For Critical (Priority 1) or High (Priority 2) incidents requiring hardware replacement, We commit to a maximum 4-hour response time to have a technician physically on-site with the spare.

- Explain any State role in spare stocking or access

Motorola Response

Comply.

The State has no role in procuring, stocking, tracking, or funding the spare inventory. Because the service is fully managed by Motorola, the State's only responsibility regarding spares is to grant the dispatched on-site technician physical admission to the PSAP control room or data center so they can access the equipment rack to verify the hardware status and swap the device.

- Show how sparing maintains required MTBF/MTTR to achieve 99.999% availability

Motorola Response

Comply.

Our sparing strategy maintains the MTBF and MTTR necessary to achieve 99.999% availability through a combination of on-site redundancy and rapid parts replacement:

Maximizing MTBF via Redundancy: All critical on-site equipment is deployed in redundant "High Availability" pairs. If one component fails, the redundant unit immediately takes over. This ensures the system does not experience a service-affecting outage, effectively masking the failure and maintaining the system's high MTBF and 99.999% availability.

Minimizing MTTR via Local Sparing: If a single device in the HA pair has a service impacting event, the system is in a vulnerable state (loss of redundancy). By utilizing spares and enforcing a strict 4-hour on-site response MTTR, the device would be rapidly replaced, and the HA pair is restored.

Operational Obligations (Post-Award):

- Maintain spare inventory at levels consistent with MTTR needs.

Motorola Response

Comply.

To ensure inventory never drops below the levels necessary to meet these MTTR targets, stock is continuously replenished. Whenever a spare is utilized to repair a system, a new spare is immediately ordered on a priority basis and delivered within 24 hours to refresh the parts depot's inventory.

- Refresh replacement stock within twenty-four (24) hours after use

Motorola Response

Comply.

Once a field technician utilizes a spare from the parts depot to repair a system, a new spare is immediately ordered to replenish the depot's stock. All parts ordered on a priority basis are delivered within 24 hours to refresh the replacement stock.

- Retain sole responsibility for restocking spare parts

Motorola Response

Comply.

Because the proposed VESTA NXT Router is delivered "as a service," Motorola retains full ownership and responsibility for maintaining all hardware components. We retain 100% responsibility for managing, tracking, and restocking the spare parts inventory.

- Track and report monthly on equipment failures requiring use of spare inventory

Motorola Response

Comply.

All equipment failures and hardware replacements are tracked within Motorola's ITSM tool, ServiceNow. Motorola provides monthly statistical reports detailing tickets opened, descriptions of the issues, resolution times, and SLA adherence.

- Adjust inventory as needed and provide documentation to the State upon request

Motorola Response

Comply.

Up-to-date inventory reports are maintained and can be provided to the State upon request.

- Identify where spares are located and maintained

Motorola Response

Comply.

Spare parts are geographically staged and maintained at our Maintenance Support Shops (MSS). The MSS is a workshop that provides repair, maintenance, tools, spare parts, and technical support for our equipment and operations.

- Use spare inventory to support the entire proposed system, adjusting as needed

Motorola Response

Comply.

Because we deliver the solution "as a service," we retain full ownership, responsibility, and maintenance obligations for all hardware and software components required to deliver the system's functionality. Therefore, our spares program comprehensively covers all delivered equipment. For example, the primary on-site equipment required at the PSAPs includes the High Availability (HA) SD-WAN Edge Devices, and we explicitly maintain spares for these at our parts depot to support the deployment.

- Replenish remote parts depots when their stock is depleted

Motorola Response

Comply.

Once the new device is configured and tested to ensure service availability, the NSOC resolves the trouble ticket. Immediately following this, a new spare is ordered and placed at the parts depot to replace the depleted stock.

- Increase spare inventory if repeated malfunctions occur.

Motorola Response

Comply.

We actively measure "Component Availability" and track component failures to uncover systemic issues. If tracking reveals that recurring malfunctions or failures are happening at a higher rate than anticipated, We will adjust and increase the spare inventory levels to ensure adequate parts are available to mitigate the repeated issue.

8.6.2 Spare Inventory at Data Centers

In addition to the spare inventory maintained at Contractor locations, the Contractor must maintain critical spare inventory on-site at each data center location. The Contractor must:

- Identify and provide documentation of critical spare inventory maintained on-site at each data center

Motorola Response

Comply.

- Add equipment to this list based on frequency and type of repair to ensure critical spare inventory is maintained on-site at all times

Motorola Response

Comply.

- Replenish spare parts inventory if required by the State in case of repeated malfunction or failure

Motorola Response

Comply.

This on-site inventory ensures immediate access to critical components needed to maintain the required system availability.

Motorola Response

Comply.

The Respondent must provide a description and/or documentation that supports the requirements in this section:

- On-site critical spare inventory at each data center.

Motorola Response

Comply.

We will maintain replacement and spare equipment parts for all delivered equipment from the date of system acceptance at each data center. Routine system maintenance operations strictly include the management of a dedicated "Spares inventory".

- Identification/documentation of inventory.

Motorola Response

Comply.

All hardware faults, on-site dispatches, and part replacements are logged and tracked via trouble tickets in our ITSM platform, ServiceNow. These records document the active components and associated spares inventory.

- Additions based on repair frequency/type.

Motorola Response

Comply.

We continuously monitor "Component Availability" and track "Component Cases" to measure failures and uncover any systemic issues. By actively tracking recurring component failures and the specific types of hardware repairs, we can dynamically adjust our inventory strategy to ensure the right equipment is added and staged to mitigate repeated failures.

- Replenishment for repeated malfunctions/failures.

Motorola Response

Comply.

Depleted spares inventory is replenished immediately. Once a spare device is used to repair a system and tested to confirm service availability, the NSOC resolves the trouble ticket immediately. To ensure critical inventory never falls below required levels, all priority-ordered parts are delivered within 24 hours of order placement.

9. Value Add and Optional Services

Respondents will describe any optional services that may enhance their product or the delivery of NG911 to the State. Particularly, this may mean the ability to deliver a hosted call handling system after the ESInet has been deployed and NG911 routing is being provided.

Motorola Response

Comply.

Motorola is offering VESTA NXT Call Handling and VESTA NXT Continuity as optional services. These options are described below in Section 9.1 and 9.2.

9.1 Call Handling Equipment (CHE) Services

The PSC would like to have insight into the options a vendor may provide for CHE. PSAPs in the State may want to move to a hosted solution or an approved solution at some point during the contract period. In order to determine the viability proposers may offer a CHE solution as an option, but it is not a firm requirement at this time.

Motorola Response

Comply.

Motorola offers **VESTA NXT call handling**, a comprehensive, cloud-native CHE solution designed to meet the evolving needs of PSAPs. Delivered as a **Call Handling as a Service (CHaaS) or Software-as-a-Service (SaaS)** model, this solution provides a highly viable and flexible path for PSAPs looking to transition to a hosted environment during the contract period.

Here is an insight into the options, architecture, and capabilities provided by this hosted CHE solution:

Cloud-Native Delivery and Subscription Model

- **All-Inclusive Subscription:** VESTA NXT call handling is offered as a fully managed subscription service that bundles the ESInet connections (SDWAN), core software, minimal on-premise hardware (like workstations and edge routers), maintenance, 24/7 technical support, and cybersecurity monitoring.
- **Evergreen Technology:** Because the software is hosted in the cloud, system updates, security patches, and new features are deployed automatically behind the scenes. This ensures PSAPs always have the most current capabilities without experiencing the downtime or capital expenses associated with cyclical on-premise system upgrades.

Scalability and Operational Flexibility

- **Comprehensive Management Information System (MIS)** which provides reporting encompassing both the Motorola call routing and call handling services.
- **Dynamic Capacity:** The cloud service has **no limit on call and position capacity**, allowing the system to automatically scale compute resources to accommodate high-demand events and call surges without requiring administrative approval.

- **Mobility and Remote Call-Taking:** VESTA NXT call handling supports remote deployments, enabling telecommunicators to process 9-1-1 calls from laptops or tablets via secure, encrypted internet connections. This capability is highly effective for mobile command vehicles, backup centers, or remote work scenarios.
- **Hot-Seating:** Telecommunicators can log into any workstation across the system—even at different physical PSAPs—and immediately access their specific user profile and home PSAP assets, such as trunks, queues, and speed-dial lists.

High Availability and Resilience

- **99.999% Reliability:** The system architecture is built to support 99.999% operational availability, utilizing geographically diverse cloud regions and availability zones.
- **ESInet architecture:** Motorola's ESInet architecture utilizes High Availability SD-WAN technology to deliver enhanced redundancy, fault tolerance, and resiliency for public safety connectivity. The carrier-agnostic design includes three network connections terminating on redundant SDWAN edge devices located at each PSAP. During normal operations, all three of these network connections remain active to deliver live traffic, preventing single points of failure and seamlessly protecting agencies from major carrier outages.
- **No Single Point of Failure:** The solution utilizes active-active failover clustering, load balancing, and multiple availability zones. If one instance or data center has a service event or degrades, core processing functionality automatically shifts to another instance without dropping active calls, losing data, or degrading performance.

Advanced NG9-1-1 Feature Options The VESTA NXT call handling platform includes a variety of advanced features that PSAPs can implement based on their specific operational workflows:

- **Multimedia and Text:** Full integration for Text-to-911 and Real-Time Text (RTT) directly within the primary call-handling workflow, processing text messages in the same queues as voice calls.
- **Media Application/Citizen Input (Video/Photos):** A cloud-based service that allows call takers to securely send a link to a caller's smartphone, granting permission-based access to stream live video or send photos directly to the PSAP.
- **Artificial Intelligence (AI) Tools:** Options include **Transcription/Translation**, which provides real-time call transcription and live language translation to reduce cognitive load. For non-emergency lines, the **Virtual Response Assistant** is an optional AI-driven bot that can triage and automate the resolution of administrative calls, freeing up telecommunicators for true emergencies.

Interoperability and Compliance

- The solution is fully compliant with **NENA i3 standards** and integrates seamlessly with existing Computer-Aided Dispatch (CAD) systems, long-term recorders, and mapping interfaces.
- To support transition periods, the solution is designed to be fully functional within legacy 9-1-1 networks (supporting legacy ALI/LDB services), ensuring continuous operations while the State or individual PSAPs migrate to an i3 NGCS and ESInet infrastructure.

Hosted CHE is preferred; to allow PSAPs an option of moving from an on-prem call handling system into the hosted CHE platform over time.

Motorola Response

Comply.

VESTA NXT call handling supports this option.

The Respondent may provide a Call Handling Equipment (CHE) solution that serves as the primary user interface for PSAP call takers and dispatchers. The CHE must be capable of receiving and managing emergency calls from the ESInet, including support for various media types such as voice, real-time text (RTT), and video. The solution must provide an intuitive graphical user interface (GUI) that displays all pertinent call information, including caller location on a map, and integrates seamlessly with other PSAP systems like Computer Aided Dispatch (CAD) and logging recorders.

Motorola Response

Comply.

Motorola proposes the VESTA NXT call handling solution, a comprehensive, cloud-native CHE solution designed to meet the evolving needs of PSAPs. The solution serves as the primary user interface for telecommunicators, is fully compliant with NENA i3 standards, and integrates seamlessly with the VESTA NXT Router Service providing call routing and location services.

Our solution satisfies the core requirements of this RFP through the following capabilities:

- **Multimedia Call Management:** VESTA NXT call handling seamlessly manages receiving and managing emergency calls from the ESInet including voice, text, and video communications. Real-Time Text (RTT) and Text-to-911 are fully integrated directly within the primary call-handling workflow and are queued and answered consistently alongside voice calls. Furthermore, the cloud-based Media Application/Citizen Input feature allows call takers to securely send a link to a caller's smartphone, granting permission-based access to stream live video or send photos directly to the PSAP.
- **Intuitive Graphical User Interface (GUI):** VESTA NXT call handling features a modern, intuitive user interface built upon extensive human-centered design research. The interface is meticulously designed to declutter the screen, utilizing a consistent left-to-right flow to minimize multitasking, reduce training time, and lower the cognitive load and mental fatigue of dispatchers.
- **Integrated Caller Location Mapping: Radius** features integrated caller location mapping, providing a powerful component that displays both the emergency event and the calling device's location. To deliver immediate, real-time situational awareness, the Radius platform plots location data from multiple sources—including standard PIDF-LO from telecommunications carriers and device-based locations—directly onto a single, unified map.

Designed as a cloud-based, tactical Next Generation 9-1-1 (NG9-1-1) mapping solution for emergency call centers, **Radius** was originally developed by RapidDeploy and recently acquired by Motorola to enhance its CommandCentral suite. It is powered by an NG9-1-1 GIS infrastructure that leverages Esri capabilities alongside the customer's authoritative GIS data, ensuring that Radius maintains full compatibility with relational GIS databases and NENA's NG9-1-1 GIS data model.

Rather than natively hosting GIS data, Radius functions as a streamlined application that consumes and aggregates GIS services hosted on the customer's or a third party's servers. Telecommunicators can easily access the Radius platform via a single URL using a standard web browser, with optimal performance on Google Chrome or Microsoft Edge.

Core Functionalities of Radius:

- **9-1-1 Location Display and Comparison:** Radius maps wireline, wireless, and VoIP calls using traditional ALI/ANI services, but supplements this with highly accurate device-based location data from Google's Android Emergency Location Services (ELS) and Apple's Enhanced Emergency Data (EED). Telecommunicators can visually compare traditional data against these supplemental locations to determine the caller's true position and track callers while they are in motion.
- **Proactive "Signals":** Through partnerships with the public safety sector, Radius enhances situational accuracy by pushing "Signals" to telecommunicators *before* a 9-1-1 call is even made. These signals include vehicle Telematics for crashes, RAVE Panic Button alerts, and mobile signals from Apple and Google. Once the telecommunicator answers the subsequent 9-1-1 call, the Signal pin automatically converts into an active Call pin on the map.
- **Enhanced Situational Awareness:** The map provides additional real-time intelligence, including traffic data from TomTom and Waze, and weather data from DarkSky. It also features robust search capabilities for addresses, points of interest, and common geodetic formats like latitude/longitude and What3Words.
- **Real-Time Transcription and Summarization:** Radius includes a Call Detail Drawer that provides a live text transcription of the active 9-1-1 call, complete with keyword highlighting, full-text search, and on-demand language translation. Furthermore, it uses this transcription stream to automatically generate and continuously update a concise, 2-3 sentence summary of the call's content to speed up critical information discovery.
- **Internal Communications:** It features an internal agency communication tool that handles text, email, and voice for emergency and non-emergency alerts, with the ability to plot these alerts directly on the map.
- **Seamless PSAP Systems Integration:** VESTA NXT call handling is designed for robust interoperability with existing PSAP ecosystems. It integrates with CAD systems using standard NENA serial spills, bi-directional IP interfaces, and EIDO conveyance. Additionally, the solution integrates with logging recorders via SIP Recording (SIPREC), fully satisfying NENA standard requirements.

Also, the signaling and media interface at the demarcation between the ESInet infrastructure and the PSAP will comply with standards-based NG911 requirements as stated in the NG911 services section and elsewhere within the technical and operational requirements. Solutions that utilize proprietary signaling and/or media across the Access Network to End Site demarcation point, or that otherwise do not comply with the technical or operational requirements specified for this demarcation point, will not be acceptable.

Motorola Response

Comply.

Motorola proposes the VESTA NXT call handling solution, which fully complies with standards-based NG9-1-1 requirements at the demarcation point between the ESInet infrastructure and the PSAP. Our solution guarantees non-proprietary, standards-based interoperability through the following:

- **NENA i3 Compliance:** The proposed solution strictly adheres to the current NENA i3 Standard for NG9-1-1 (NENA-STA-010.3f-2021). Furthermore, it adheres to the NENA Next Generation 9-1-1 PSAP Requirements (NENA-REQ-001.1.2-2018).
 - **Standardized Ingress:** 9-1-1 calls ingress directly into the VESTA NXT call handling via the NGCS infrastructure. The system is fully capable of accepting 9-1-1 SIP calls via an ESInet using industry-standard protocols.
 - **Non-Proprietary Interfaces:** The VESTA NXT call handling solution does not utilize proprietary signaling or media across the Access Network to End Site demarcation point. We confirm full compliance with providing a non-proprietary, standards-based solution to ensure interconnectivity and interoperability without the limitations of proprietary protocols.
-

9.2 ESInet and NGCS backup system

The PSC would also like to understand the options a vendor may provide to increase the diversity and redundancy of the system. This may be a tertiary alternative that could be utilized in the event of the primary system or transport failure.

Motorola Response

Comply.

Our proposed solution for the Commission provides a robust and exceptionally resilient ESInet backbone, ensuring that public safety operations remain uninterrupted even during service events impacting the ESInet or "last mile" transport network.

The design improves system diversity by utilizing cutting-edge SD-WAN technology alongside national MPLS carriers and multiple Broadband carriers.

Triple Path Diversity & SD-WAN Technology

To protect our proposed ESInet connection, the architecture provides triple path diversity for all PSAP controllers, utilizing one national carrier MPLS circuit and two broadband circuits:

- **Terrestrial Primary/Secondary Circuits:** Physically diverse terrestrial MPLS and Broadband circuits (copper or optical fiber) serve as the primary and secondary connections.
- **Tertiary Circuit:** Terrestrial broadband or wireless broadband (e.g Low Earth Orbit (LEO) Satellite) provides a completely independent tertiary path.
- **SD-WAN Management:** Advanced Software Defined Wide Area Network (SD-WAN) edge devices terminate at each call handling host location, seamlessly bonding these diverse connections to provide instant, automated failover.

Optional Backup: VESTA NXT Continuity

If the Commission wishes to explore enhanced protections against the physical destruction of a PSAP (e.g., a tornado) or total local network failure, we offer VESTA NXT Continuity as an option. This cloud-based, "lite" backup system operates entirely independent of the local ESInet and requires zero backroom equipment. If the primary call handling system fails, telecommunicators can seamlessly transition to process live 9-1-1 calls via any available internet connection (including public Wi-Fi or LTE) with the following capabilities:

- **Native i3 Call Handling:** Fully NENA i3-compliant, requiring the call to be delivered via an i3 IP network.
 - **Rapid Deployment:** Requires minimal training and supports an unlimited number of operator positions.
 - **Comprehensive Situational Awareness:** Provides full caller location displays, including supplemental caller location data.
 - **Cloud-Native Logging:** CDR and call audio are securely captured and stored in the cloud via CommandCentral Evidence based upon the PSAP storage retention policy, ensuring total evidentiary continuity.
-

10. Use Case Examples for Use with Response

10.1 Instructions

The following diagrams depict the NG911 system from a functional view. These Use Case scenarios provide Respondents the opportunity to demonstrate the traffic flow and performance perspectives of their proposed system. The Use Cases are designed to present a basis for validation of responses to the requirements of the RFP and will be used as a basis for evaluation of the delivery of traffic from caller to PSAP.

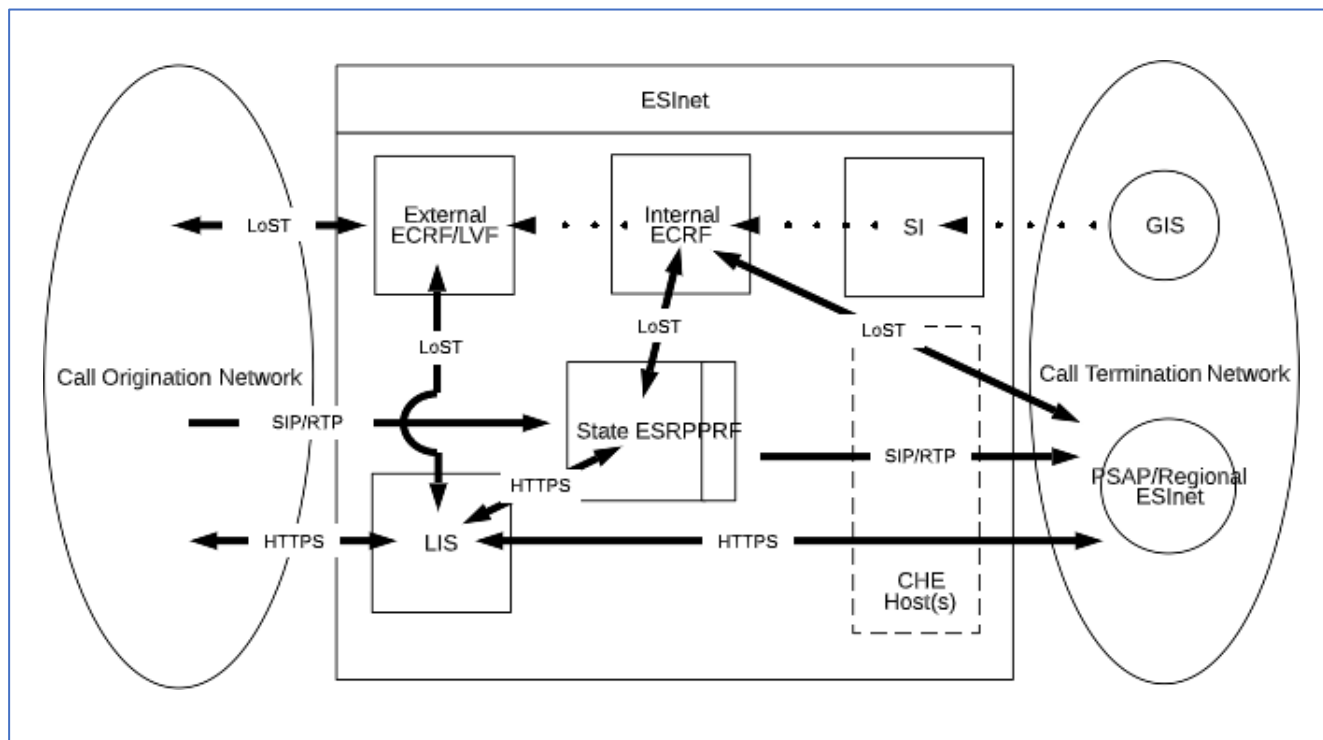


Figure 5-3: High Level NENA i3v3 Architecture

High-Level Use Case and Overall Expectation

The first expectation is for the Respondent to offer a narrative of how their proposed solution will meet the functionality depicted in the above diagram.

Respondents must:

- Describe how traffic flows from the call origination network, through the core to the PSAP in step-by-step fashion.
 - At each functional element, a description shall be provided to discuss how the traffic flow is being modified or adjusted due to additional data between functional elements.
 - At each functional element, a description shall be provided to identify how the system is managed and how alerts of disruptions or incidents will automatically notify the NOC.
 - At each functional element, a description of how the interface between the functional elements will be utilized.
 - Demonstrate how the system will handle the use case presented and discuss the operation, including which partner(s) (Prime or Subcontractor) would be responsible for ingress, core, and egress.
 - Identify the bandwidth available and options to manage and monitor bandwidth between functional elements and for the entire platform.

Motorola Response

Comply.

Functional Elements Diagram Per "Availability Region"

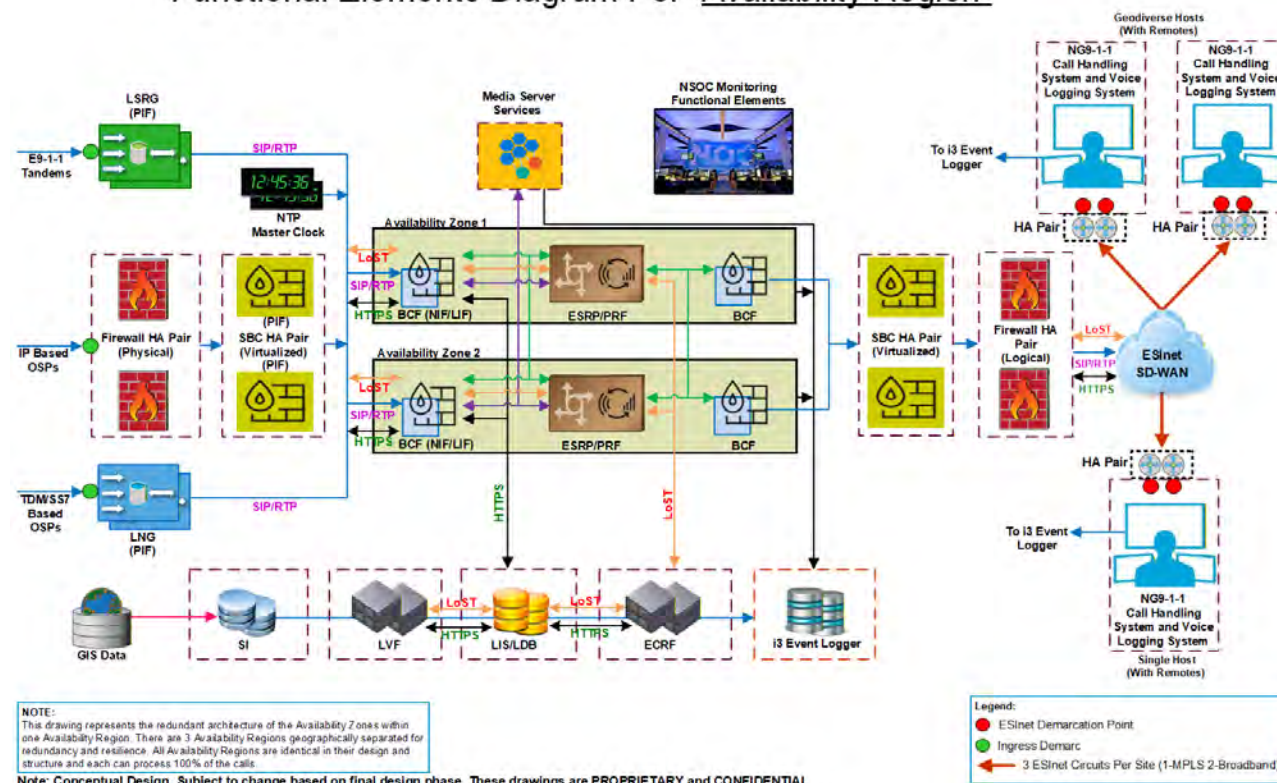


Figure 5-4: Functional Elements Diagram

Step-by-Step Traffic Flow, Functional Elements, and Interfaces

Reference the System Architecture Diagram above, detailed explanations and call flows are provided in subsequent paragraphs:

1. Call Ingress & LNG / BCF

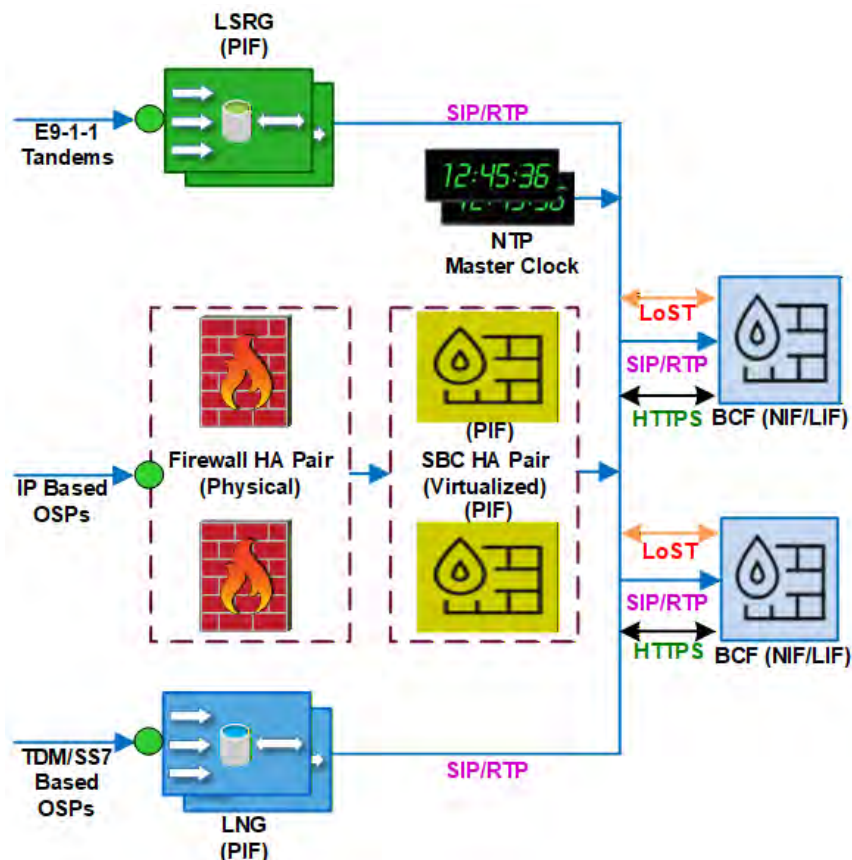


Figure 5-5: Call Ingress, LNG and BCF

- **Traffic Flow:** A 9-1-1 call originates from a wireless, wireline, or VoIP OSP and arrives at the network POI. If the call arrives via legacy TDM (analog), it connects to the LNG. If it arrives via IP utilizing **SIP/RTP**, it goes directly to the ingress BCF, which includes SBC and firewalls.
- **Modifications via Additional Data:** The LNG converts TDM traffic to **SIP**. If the OSP does not provide the caller's location with the call, the system queries the LDB using **HELD** to acquire the location and inserts it into the SIP header as a (PIDF-LO). The BCF classifies the call type and modifies the Layer 3 IP header by adjusting DSCP values (e.g., tagging voice packets with Expedited Forwarding priority 46) to ensure QoS.
- **System Management & NOC Alerts:** Our NSOC actively monitors these edge devices using network probes. If an LNG or BCF node has a service event or if traffic thresholds are impacted, the NMS automatically generates an actionable alarm and opens a trouble ticket in the ITSM tool (ServiceNow), alerting the NSOC within 15 minutes for critical outages.
- **Interface Utilization:** TDM interfaces (ISUP/CAMA) are utilized on the OSP-facing side of the LNG, while **SIP** and Real-Time Transport Protocol (**RTP**) are utilized on the core-facing side. IP based traffic uses SIP/RTP.

2. Emergency Services Routing Proxy (ESRP), ECRF & LVF

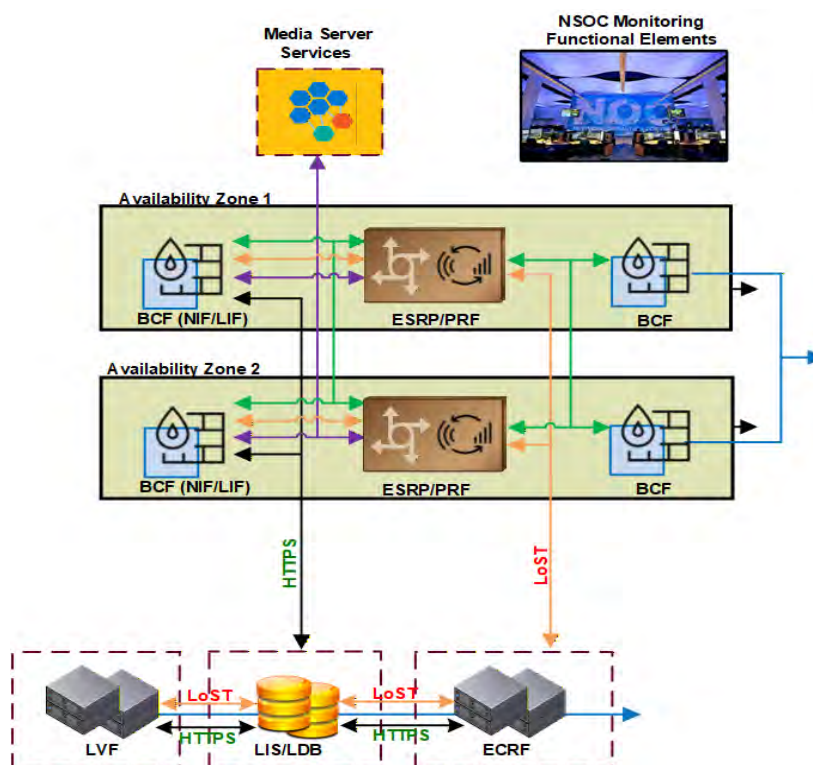


Figure 5-6: ESRP, ECRF and LVF

- **Traffic Flow:** The **SIP** INVITE is received by the ESRP, which acts as the primary call routing engine within the NGCS. The ESRP must determine the appropriate PSAP destination.
- **Modifications via Additional Data:** The ESRP extracts the PIDF-LO location data and sends a **LoST** query to the ECRF. The ECRF compares the location against authoritative GIS boundaries and returns the specific Uniform Resource Identifier (URI) of the destination PSAP back to the ESRP, modifying the call's routing path.
- **System Management & NOC Alerts:** The ESRP and ECRF are deployed as redundant microservices in a multi-cloud architecture. The NSOC monitors **LoST** transaction processing times and **SIP** error codes. If an ECRF database fails to synchronize or an ESRP instance becomes unreachable, the system automatically fails over to a redundant node, and the NSOC is alerted to investigate the specific application error.

Interface Utilization: The ESRP utilizes the **LoST** protocol (RFC 5222) over secure **HTTPS** to interface with the ECRF. The proposed **ECRF/LVF** solution provides for error handling, discrepancy management, default routing, and logging. The ECRF/LVF will respond to any validation request originating from an authorized source. Given that a validation query is the same as a routing query, we use our solution for both ECRF and LVF implementations. We will deploy the LVF instance(s) of our LVF / ECRF application separately from the ECRF instances to ensure that bulk validations do not affect call routing.

3. PRF

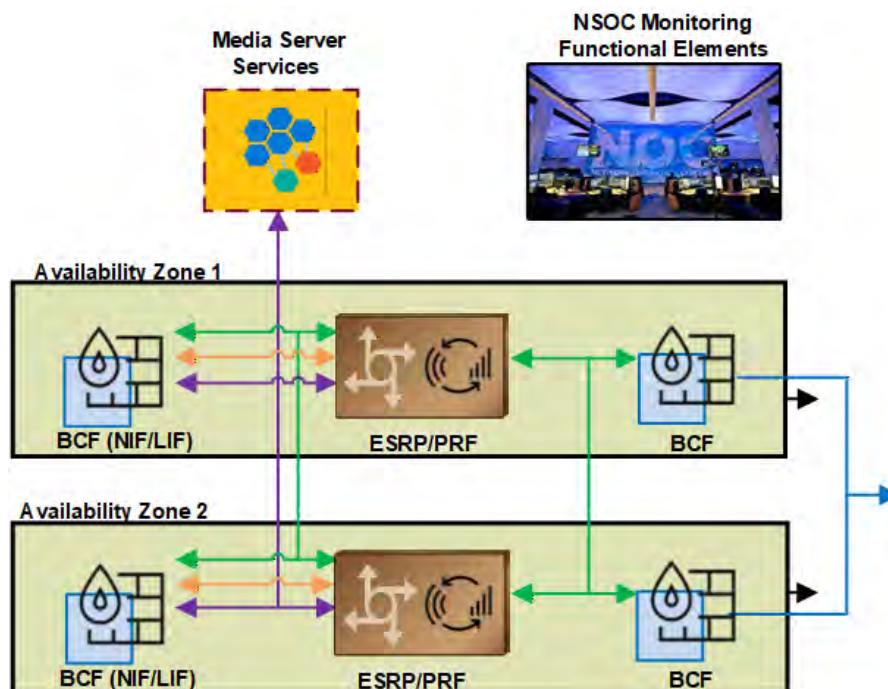


Figure 5-7: PRF

- **Traffic Flow:** Before the ESRP finalizes the route, it consults the PRF to apply any agency-specific routing rules.
- **Modifications via Additional Data:** The PRF evaluates additional contextual data, such as time-of-day, the current queue state of the destination PSAP, or known non-operational . If the primary PSAP is busy or abandoned, the PRF modifies the route and instructs the ESRP to divert the call to a predetermined alternate URI.
- **System Management & NOC Alerts:** PSAP administrators and the NSOC manage PRF rules via the CWP. If an automated policy diversion occurs (e.g., an overflow route is triggered), the system logs the event and visually alerts stakeholders via the portal's live map, turning the affected PSAP's status icon yellow or red.
- **Interface Utilization:** The ESRP utilizes **internal SIP** and APIs to query the PRF and evaluate the PRR stored in the policy database.

4. Egress BCF & PSAP Delivery

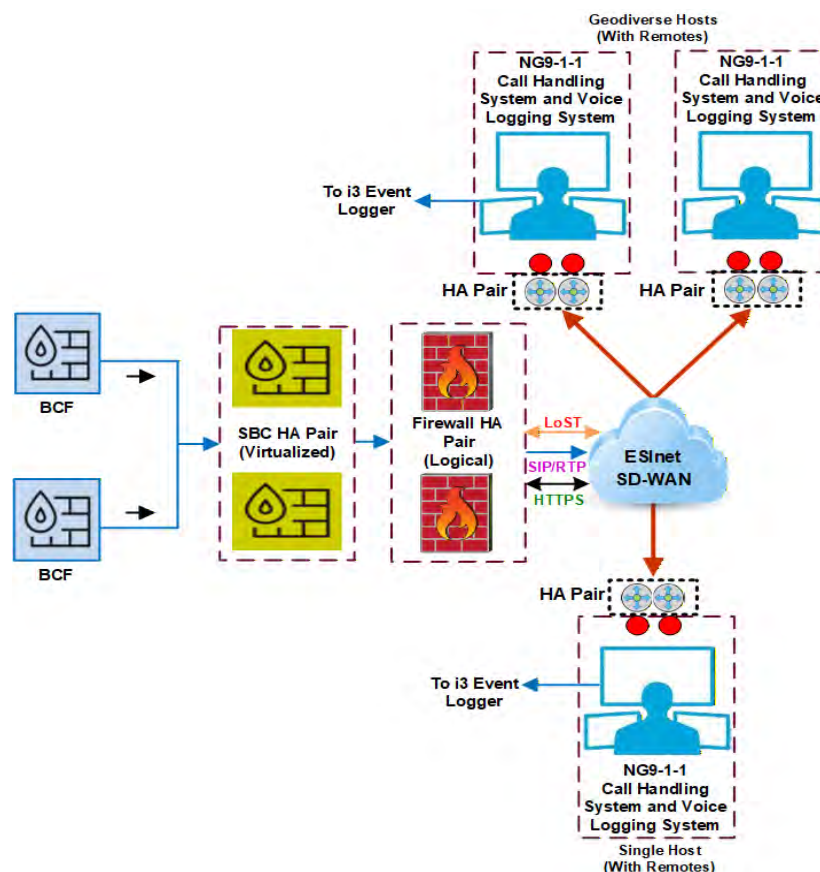


Figure 5-8: Egress BCF and PSAP Delivery

- **Traffic Flow:** The ESRP forwards the **SIP** INVITE and **RTP** media stream through the egress BCF and across the ESInet to the call handling host equipment associated with the destination PSAP.
- **Modifications via Additional Data:** The egress network maintains the DSCP QoS markings applied earlier to ensure voice packets are prioritized over administrative data across the ESInet.
- **System Management & NOC Alerts:** Active network probes continuously monitor the ESInet routers at the call handling host demarcation point. If one network path drops, dynamic routing protocols (e.g. BGP) and the SDWAN overlay will automatically reconverge traffic to a redundant network path in less than 54 milliseconds, while simultaneously triggering an automated NSOC ticket regarding the degraded network path.
- **Interface Utilization:** The egress interface utilizes **SIP** for call setup/teardown and **RTP** for two-way audio and Real-Time Text (**RTT**) delivery directly to the PSAP's CHE.

5. LDB, Location Information Service (LIS) and SI.



Figure 5-9: LDB, LIS and SI

- **Traffic Flow:** Our **LDB** serves as both a legacy ALI database and as a **LIS** in an i3 NG9-1-1 environment and is included architecture to fully replace the existing ALI database and enable smooth transition to NG9-1-1.
The **SI** will provide QA/QC, GIS aggregation, and administration to support the State's data provisioning needs for the **ECRF/LVF**. Our **SI** is designed to allow a single statewide dataset or multiple GIS users to upload mission-critical spatial data, that is then automatically validated, in support of the required NG9-1-1 format and functionality for public safety.

Contractor responsible for Core Ingress and Egress

Motorola is the sole contractor responsible for all aspects of the service including ingress, core and egress.

- **Ingress:** Responsible for the OSP interconnection infrastructure. We provide the physical POIs, aggregate the incoming traffic, and provide the media conversion (LNGs) to hand off SIP traffic to Motorola's core.
- **Core:** Retains overall responsibility associated with all functional elements within the NGCS as well as the 24x7x365 NSOC.
- **Egress:** Responsible for the ESInet transport and terminating SDWAN edge appliances carrying the traffic from the NGCS core to the call handling host facilities.

Bandwidth Availability, Management, and Monitoring

- **Availability:** Bandwidth is calculated to support 125% of call volumes and is engineered using NENA's baseline formula (e.g., *2 Mbps per PSAP + 2 Mbps per call-taker position equipped for video*). The network is scalable to support 50% bandwidth growth without requiring hardware replacements.
- **Management:** Bandwidth is managed using DiffServ and DSCP tagging to implement strict traffic shaping. Real-time voice (RTP) is placed in a high-priority queue (Expedited Forwarding), SIP signaling in a secondary queue, and all other data in a "Best Effort" queue to ensure critical audio is never dropped during bandwidth congestion.
- **Monitoring:** Bandwidth utilization, latency, jitter, and packet loss are continuously monitored by the NSOC. State and PSAP administrators can monitor system health and SLA performance in near real-time using the CWP.

- Describe the performance expectations of the system and explain how performance is guaranteed for legacy 911 across the entire system to egress to a legacy PSAP.
 - Identify how systems operate in a "normal" state.
 - Identify how systems operate in an "abnormal" condition.

- Demonstrate how the platform will operate in a "fail" condition.

Motorola Response

Comply.

Performance Expectations and Guarantees for Legacy 9-1-1

The system is engineered to provide 99.999% operational availability from end to end, with no single point of failure. To guarantee performance for legacy 9-1-1 traffic traveling across an IP-based NGCS network to a legacy PSAP, the system utilizes specific gateways:

- **Ingress:** Legacy Network Gateways (LNG) or LSRGs interface with Time Division Multiplexing (TDM) or analog connections from OSPs, converting the legacy traffic into SIP formats for the core network.
- **Location:** The system queries the LDB, which acts as a legacy ALI database, to pull location data from legacy Mobile and VoIP Positioning Centers before routing.
- **Egress:** If a PSAP has not yet upgraded its CHE to an i3-compliant system, a LPG is deployed at the network edge to perform an IP-to-analog handoff.

Performance is defined through SLAs. These SLAs require that voice quality maintain a MOS of 4.0 or higher (or PMOS above 3.5), network traffic convergence occurs in under 54 milliseconds, and the network bandwidth is scaled to handle 125% call volumes.

Operation in a "Normal" State:

- **Active Load Balancing:** Under normal conditions, 9-1-1 calls and data are actively load-balanced across multiple geographically diverse instances within a multi-cloud architecture.
- **Continuous Routing:** Traffic enters through the BCF, where the Emergency Services Routing Proxy (ESRP) queries the ECRF and PRF to determine the proper destination based on the caller's location and agency policies.
- **Active Circuit Utilization:** All circuits are used to process live traffic via SD-WAN to ensure they are available and capable of supporting live traffic.
- **QoS:** Voice traffic (RTP) is tagged with DSCP markings (e.g., Expedited Forwarding priority 46) to ensure it receives priority over all other administrative data on the network.

Operation in an "Abnormal" Condition:

Abnormal conditions include scenarios like sudden call volume spikes, PSAP queue overloads, or network degradation (e.g., high packet loss or jitter).

- **Automated Policy Routing (Busy/Overflow):** If the primary PSAP is overwhelmed and cannot answer, the PRF detects the condition. If a call goes unanswered for a configurable amount of time (e.g., 60 seconds), the system triggers "Overflow Call Routing" and dynamically pulls the call back to deliver it to a predefined alternate destination.
- **Traffic Shaping & Reconvergence:** If network degradation occurs, dynamic routing protocols (such as OSPF and BGP) utilize Bidirectional Forwarding Detection to detect the fault with low overhead. The system will automatically reconverge and reroute traffic around the functional elements or network links, negatively impacting the MOS score.

- **Cybersecurity Containment:** In the event of a TDoS attack, the BCF can identify abusive caller profiles and the PRF can automatically route those specific calls into a low-priority queue or an automated attendant, keeping the primary queues clear for legitimate 9-1-1 emergencies.

Operation in a "Fail" Condition:

Fail conditions cover the total loss of a hardware component, network link, or an entire physical facility.

- **Automated Sub-Second Failover:** Because the system utilizes an Active/Active redundancy model, the failure of a single router, server, or egress network path will not cause a system outage. Dynamic routing protocols, SDWAN and Fast Reroute (FRR) technologies detect the failure and automatically failover to redundant network paths or redundant elements, mitigating the failure so that no 9-1-1 calls are dropped.
 - **PSAP Abandonment:** If an entire PSAP facility suffers a catastrophic failure or requires immediate evacuation (e.g., due to fire, flood, or gas leak), administrators can invoke the "PSAP Abandonment" via the CWP. This automatically reroutes all incoming calls to pre-defined contingency destinations.
 - **"OPTIONAL "Backup:** In the case of a complete failure of the local ESInet or primary CHE, we offer an optional fallback through our VESTA NXT Continuity solution. This solution is a cloud-based, browser-accessible mobile call-handling service that can function securely over any standard internet connection or public Wi-Fi, effectively circumventing the compromised local infrastructure.
-

- Describe how security is implemented across the system while maintaining the performance guarantees expected to egress to a legacy PSAP.
 - Identify how DDoS and TDoS events are mitigated.
 - Identify how security events are mitigated at each component throughout the system, including incidents that derive from the OSP, the PSAP and other ESInets.

Motorola Response

Comply.

System Security and Performance Guarantees (Legacy PSAP Egress): We build security into the system from the ground up as a core functional element rather than an aftermarket add-on, explicitly planning security and availability together to align their impact zones. The system employs a "defense-in-depth" and "zero-trust" architecture based on NIST SP 800-53 and NENA NG-SEC standards.

To secure the network while maintaining stringent performance for calls delivered to a legacy PSAP, the system relies on the following mechanisms:

- **BCF:** All calls entering or exiting the NGCS must pass through a BCF, which includes SBC and firewalls. The SBC acts as an Application Layer Gateway for SIP traffic, while firewalls utilize a strict "deny-all" posture that only permits authorized 9-1-1 traffic.
- **Performance Maintenance:** Even with these security inspections, the BCF and core network maintain performance assurances by leveraging DSCP QoS markings. Voice packets (RTP) are tagged with high-priority Expedited Forwarding to ensure they are prioritized over administrative data, preserving a MOS of 4.0 or higher.

- **Legacy Handoff:** The secured, high-priority IP traffic traverses the ESInet and is handed off to the legacy PSAP via a LPG, which performs the required IP-to-analog conversion.

Mitigation of DDoS and TDoS Events: The system protects the 9-1-1 network from malicious floods of traffic through distinct, multi-layered strategies for both data-level and telephony-level attacks:

- **DDoS:** The firewalls and SBCs are capable of detecting unusual types, origins, or volumes of incoming IP packets and blocking them. The DDoS mitigation strategy includes network-level mitigation, IDS/IPS, traffic scrubbing, and rate limiting. Furthermore, the system leverages enhanced cloud-provider protections, offering always-on traffic monitoring, adaptive real-time tuning, and rapid response mitigation.
- **TDoS and Non-Service Initiated (NSI) Calls:** The system evaluates incoming calls and assigns confidence levels to identify potential malicious traffic. If an attack is suspected, the PRF utilizes directed queuing to quarantine abusive callers by automatically routing them to a low-priority call queue or automated attendant, keeping the primary 9-1-1 queues clear for legitimate emergencies. To protect the core routing engine from being overwhelmed, SBCs are configured to immediately reject SIP calls presenting with abnormal headers. Additionally, the NSOC will notify the OSP generating the attack so the OSP can implement upstream mitigation strategies.

Mitigation of Security Events Across Specific Components: The 24x7x365 NSOC uses SIEM tools to continuously monitor system logs and network traffic across the entire ecosystem. When a threat is detected, the NSOC executes an incident response plan to contain, eradicate, and recover from the breach.

Security events are mitigated differently depending on where they originate:

- **Incidents from OSPs (Ingress):** All OSP traffic enters the network through the ingress BCF. The SBC provides firewall-like security specifically for call signaling and media streams, ensuring no transport layer information simply "passes through". If malicious traffic attempts to enter, the BCF firewalls block it, and connections are secured using TLS or IPsec VPN tunnels.
- **Incidents from PSAPs (Egress):** Because PSAPs often present the greatest cybersecurity threat to the broader network, the architecture isolates and contains threats at the local PSAP level. The network is deeply segmented so that each PSAP is isolated from other PSAPs, preventing lateral movement by attackers.
- **Incidents from Other ESInets (Peers):** When interconnecting with neighboring jurisdictions or third-party networks, the system enforces strict authentication. It requires mutual authentication using digital certificates issued by a vetted Public Key Infrastructure (PKI), such as the NENA PSAP Credentialing Authority (PCA). This ensures that only trusted entities can establish connections with the core network.

-
- Describe how 911 data is delivered to the logging and reporting system to be accessed by a PSAP.
 - Identify how databases operate.
 - Explain how recording systems are implemented to accommodate local recording and to accommodate hosted recording.
 - Explain how logging is collected and accessed for legacy CDR and i3 logging.

Motorola Response

Comply

Delivery of 9-1-1 Data to the Logging and Reporting System for PSAP Access. The delivery of 9-1-1 data to logging and reporting systems is designed to provide comprehensive, end-to-end visibility of an emergency call. The system aggregates data from multiple sources:

- **Core Network and ESInet Data:** The i3 Event Logger continuously captures payload metadata and logs 24x7x365 from all functional elements within the NGCS and the ESInet.
- **Text-to-9-1-1 Data:** The reporting module pulls text session data directly from the TCC, capturing message transcripts and agent response times.
- **Call Handling Data:** The Management Information System (MIS) collects CDR directly from the PSAP's local CHE.

How Databases Operate: Once captured, this data is buffered, securely stored, and made available in near real-time. PSAP administrators access this data through a secure CWP, which provides a single, unified web-based interface to run dynamic analytics, view dashboards, and generate both standard and ad-hoc reports from any internet-connected device.

Implementation of Recording Systems (Local vs. Hosted) Recording systems capture the audio and data of a 9-1-1 call processed by a call handling system.

- **Local Recording:** For agencies that prefer or already have local logging recorders, the call handling system interfaces directly with the on-premise local recording equipment. The CHE deployed at the PSAP can provide an analog output for audio at the telecommunicator's workstation (similar to traditional voice recording). Alternatively, the equipment provider can supply a span port off their local area network (LAN) switch to deliver an IP-based output directly to the agency's existing local call recorder.
- **Hosted Recording:** For agencies that prefer or already have hosted logging recorders, the call handling system interfaces directly with the hosted recording equipment. The equipment provider can supply a span port off their local area network (LAN) switch to deliver an IP-based output directly to the agency's hosted call recorder.

Collection and Access for Legacy CDR and i3 Logging: To provide a complete picture of PSAP performance, the service combines legacy and Next Generation data access:

- **Legacy CDR Collection:** CDRs are extracted directly from the local call handling system. This output is stored in its original format to preserve the chain of custody for auditing and legal defensibility.
- **i3 Logging Collection:** The i3 logger acts as a transactional event logger, capturing SIP messaging (INVITEs, REFERs, SIP errors) and queries/responses (HELD, LoST) as they traverse the NGCS functional elements.
- **Unified Access:** Users do not need to log into separate systems to view legacy CDR and i3 logs. The web-based reporting suite integrates both datasets to provide End-to-End Reporting. Through the Eclipse Analytics reporting portal, an authorized user can search by date, time, or callback number to see a chronological list of calls. Clicking on a specific Call ID allows the user to drill down into the exact sequence of i3 network events alongside the legacy CDR data, which can then be exported for deeper analysis.

- Describe how calls may be transferred between NG PSAPs.
 - Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on the same NG911 system.
 - Explain how the NG PSAP to NG PSAP transfer will be triggered, and how the call will move from one PSAP to another on a different NG911 system.
 - Describe how transfers are logged and how the data is logged.
 - Discuss the data that is transferred to the receiving PSAP.
 - Explain how logging is collected and accessed for legacy CDR and i3 logging

Motorola Response

Comply.

How Calls are Transferred Between NG PSAPs In a Next Generation 9-1-1 (NG9-1-1) environment, call transfers and conferences are executed using SIP signaling over the ESInet. Instead of relying on legacy analog trunks, PSAPs can seamlessly conference or transfer a call to another PSAP by directing the NGCS to add a secondary URI to the session.

Triggering a Transfer on the *Same* NG9-1-1 System When a call is transferred to a PSAP on the same NG9-1-1 system, the process operates as follows:

1. **The Trigger:** The transfer is initiated by the telecommunicator using a shortcut button or dial directory contact within their Call Handling System (CHS).
2. **The Movement:** This action prompts the CHS to send a SIP REFER request (or a conference request) to the NGCS BCF. The request contains the unique identifier or URI of the destination PSAP. Because both PSAPs reside on the same network, the NGCS routing proxy simply accepts the request, bridges the connection across the shared ESInet, and delivers the SIP INVITE to the secondary PSAP.

Triggering a Transfer to a *Different* NG9-1-1 System When transferring a call to a PSAP operating on a completely different NG9-1-1 system, the initiation trigger is the same (the call taker utilizes their CHS interface), but the network movement requires external interoperability:

1. **outing Determination:** If the destination URI is not already pre-configured, the originating NGCS may send a LoST query to the ECRF to determine the proper routing URI for the outside jurisdiction. To facilitate this, NGCS providers share PSAP boundaries or utilize a hierarchical "Forest Guide" to locate the correct external agency.
2. **The Movement / NNI:** The call is transmitted across a Network-to-Network Interface (NNI). The NNI is a mutually agreed-upon, secure integration point that governs how peer NGCS networks exchange calls, features, and protocols. The SIP REFER and INVITE messages are routed across the ESInet, through the NNI, and into the peer NGCS network, which then delivers the call to the receiving PSAP.

Transferred to the Receiving PSAP To ensure the receiving PSAP has full situational awareness, NG9-1-1 transfers utilize an EIDO to convey incident and call information.

- When the SIP INVITE or REFER message is sent to the receiving PSAP, it includes specific Call-Info headers containing the NENA Call Tracking ID, the Incident ID, and a reference link (URI) to the EIDO.

- **Payload Contents:** At a minimum, the EIDO contains the information received during the original call, including the 9-1-1 calling device's location, the callback number, and any additional subscriber data.
- **Call Notes:** The NENA standard for EIDO also allows for additional information acquired by the initial telecommunicator—such as a more precise incident location or manual call notes—to be packaged into the EIDO and transferred. (Note: The ability to pass manual call-taker notes depends on the specific software capabilities of the local CHE deployed).

How Transfers and Data are Logged: Transfers are logged thoroughly at the network level by the NGCS i3 Event Logger. Operating as a "transaction logger," it captures and timestamps all SIP messaging metadata (such as INVITES, REFERS, and SIP errors) as well as data queries (like HELD for location and LoST for routing) as they traverse the network.

Motorola's Eclipse reporting system provides Summary Reference Sheet reports for inter-PSAP transfers. Included in these reports is a 911 Transfers page report with detailed information on Total 911 Transfers, % of 911 calls transferred, Average time till transfer, Top transfer targets, transfers by cell sector, and much more details

Collection and Access for Legacy CDR and i3 Logging: To provide a complete picture of PSAP performance, the system combines legacy and Next Generation data access:

- **Legacy CDR Collection:** CDRs are collected directly from the local call handling system. This output is stored in its original format to preserve the chain of custody for auditing and legal defensibility.
- **i3 Logging Collection:** The i3 logger acts as a transactional event logger, capturing SIP messaging (INVITES, REFERS, SIP errors) and queries/responses (HELD, LoST) as they traverse the NGCS functional elements.
- **Unified Access:** Users do not need to log into separate systems to view legacy CDR and i3 logs. The web-based reporting suite integrates both datasets to provide End-to-End Reporting. Through the Eclipse Analytics reporting portal, an authorized user can search by date, time, or callback number to see a chronological list of calls. Clicking on a specific Call ID allows the user to drill down into the exact sequence of i3 network events alongside the legacy CDR data, which can then be exported for deeper analysis.
- **Raw Data Extraction:** For deep analysis or auditing, authorized users can use the Eclipse Reports and Data viewer to search and extract raw i3 SIP logs (searchable by date, time, or callback number) and the Eclipse Raw Data viewer to pull the legacy CDRs in their original formats. These logs can be viewed chronologically and exported into PDF, HTML, Excel, or CSV formats.

-
- Describe any areas where the "span of control" on enforcement of diversity, redundancy, policies, procedures or any other automated or manual function that would limit the overall success of a call reaching a call taker is within the system.
 - Explain the limitations with the proposed system in a clear manner so that the evaluation team, and the State have a clear understanding of what is being proposed.
 - Gaps and limitations do not disqualify or eliminate a proposal; on the contrary an open and honest response will allow these types of issues to be documented and will lead to a collaborative plan to remediate.

Motorola Response

Comply.

To provide an open and honest assessment; as requested by the State of Nebraska of the proposed Next Generation 9-1-1 (NG9-1-1) system, it is important to clearly define Motorola's "span of control". While Motorola provides a highly redundant, NGCS and ESInet architecture supporting 99.999% operational availability. There are specific boundaries, dependencies, and external factors that can limit the overall success of a call reaching a call taker.

Here are the key limitations and areas that fall outside of, or constrain, the system's span of control:

1. OSPs and Ingress Limitations: Motorola's span of control begins after the 9-1-1 call arrives at the NGCS POI. The system is heavily dependent on the OSPs (wireless, wireline, and VoIP carriers), which presents the following limitations:

- **Location Delivery:** The NENA i3 end-state architecture assumes that OSPs will provide the caller's location at the time the call is presented to the NGCS for routing. However, OSPs are currently under no mandate by the FCC to deliver location with the call. Furthermore, the FCC does not dictate the technology OSPs must use to determine location. If an OSP fails to send accurate location data, the system must spend additional time querying the LDB to retrieve it, which can cause slight delays or require fallback routing.
- **Upstream Outages and Attacks:** If an OSP experiences a network outage, a severed fiber cable, or a massive TDoS attack within their own network, the traffic may be dropped or saturated before it ever reaches Motorola's ESInet. While Motorola's Network Security Operations Center (NSOC) monitors for these attacks and will notify the OSP so they can implement upstream mitigation, Motorola cannot control the OSP's span of control.

2. The "Last Mile" and Physical PSAP Diversity (Egress Limitations) Motorola's span of control ends at the physical demarcation point at the call handling system host location, which is the call handling system-facing port of the ESInet egress network termination router.

- **CPE:** Any service interruptions, audio quality degradation, or delays caused by the local CHE, local area network (LAN), or PSAP-owned firewalls are outside our system's control.
- **Lack of Physical Diversity:** While Motorola enforces carrier and network diversity to prevent single points of failure, true physical diversity is sometimes limited by local infrastructure. For example, using different carriers does not always guarantee path diversity if those carriers share common network paths, trenches, or utility poles leading into the PSAP. If a PSAP building only has a single physical entrance for cabling, a physical incident (like a severed conduit in the parking lot) could compromise multiple network circuits simultaneously.

3. GIS Data Accuracy and Provisioning Location-based routing is only as reliable as the Geographic Information System (GIS) data supporting it.

- **Authoritative Control:** While Motorola provides the SI tools and rigorous Quality Assurance/Quality Control (QA/QC) to detect gaps, overlaps, and errors, Motorola does not own or author the GIS data. The local addressing authorities, the State or contracted entities that maintain the authoritative GIS data.
- **Routing Limitations:** If the provided GIS data is incomplete, unsynchronized, or contains uncorrected errors, the ECRF may not be able to geospatially route the call. In these scenarios, the system is limited to falling back to default routing, which reduces the precision of the call routing.

4. Legacy Interoperability and CHE The successful delivery of NG9-1-1 features (e.g. multimedia, video, and advanced data) requires the PSAP to have a NENA i3-compliant call handling system.

- **Legacy Gateways:** If a PSAP has not upgraded its equipment, the system must utilize LPGs to convert the IP signal back to analog (CAMA) format. This strips the call of its advanced i3 capabilities, meaning telecommunicators cannot receive IP-based multimedia or real-time text directly through the standard voice path.
- **Neighboring Jurisdictions:** When transferring a call to a neighboring county or state that operates on a legacy router or a different standard, the rich data payload cannot be delivered during the transfer if the receiving agency's system cannot process it. This forces the telecommunicator to verbally relay information, adding time to the response.

5. Human-in-the-Loop and Policy Management The NGCS PRF relies on rules established by the PSAPs.

- **Misconfigurations or Manual Failures:** If PSAP administrators configure conflicting routing rules, or if they fail to activate a "PSAP Abandonment" during a facility evacuation, calls may route to an unmanned PSAP and sit in a queue until an automatic "ring-no-answer" overflow timer is triggered.
-

10.2 Additional Examples

The following diagrams serve as an example of how a Respondent shall answer the use case questions. Diagrams may be necessary with step-by-step demonstration callouts to document the overall traffic flow for the system. Respondents are encouraged to use their own diagram(s) to illustrate the traffic flow from end to end.

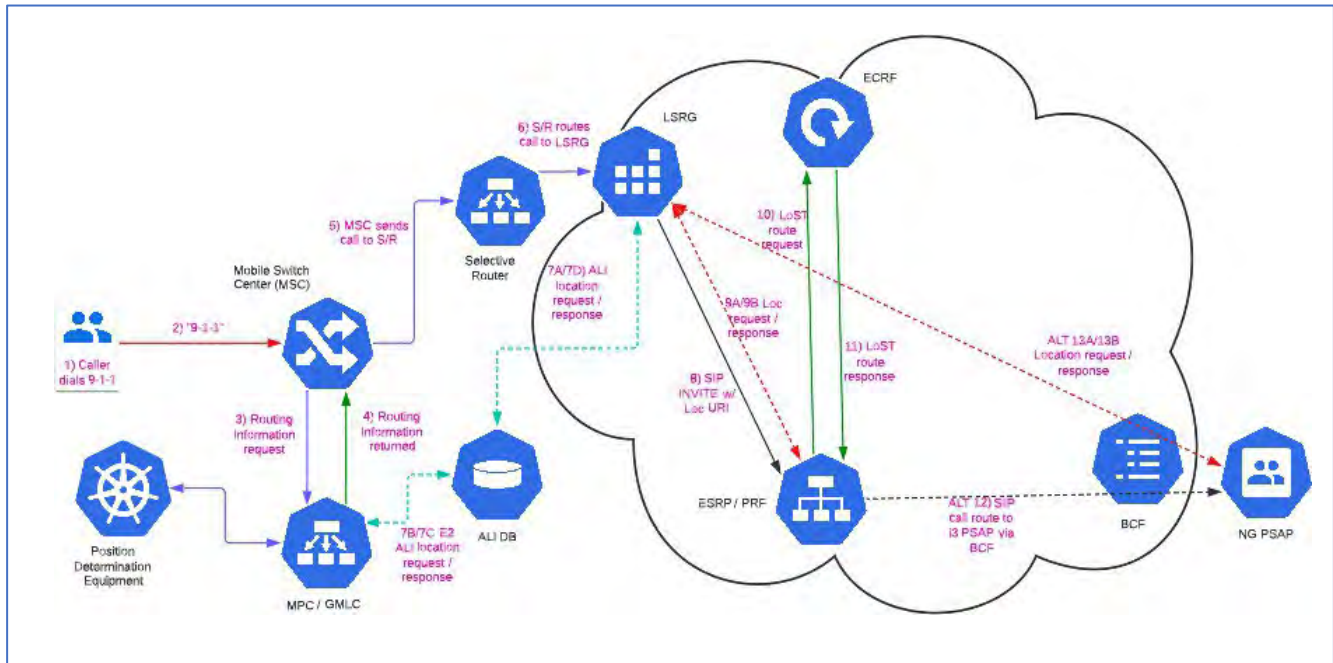


Figure 5-10: NENA Call Flow Scenario 1

Motorola Response

Understood

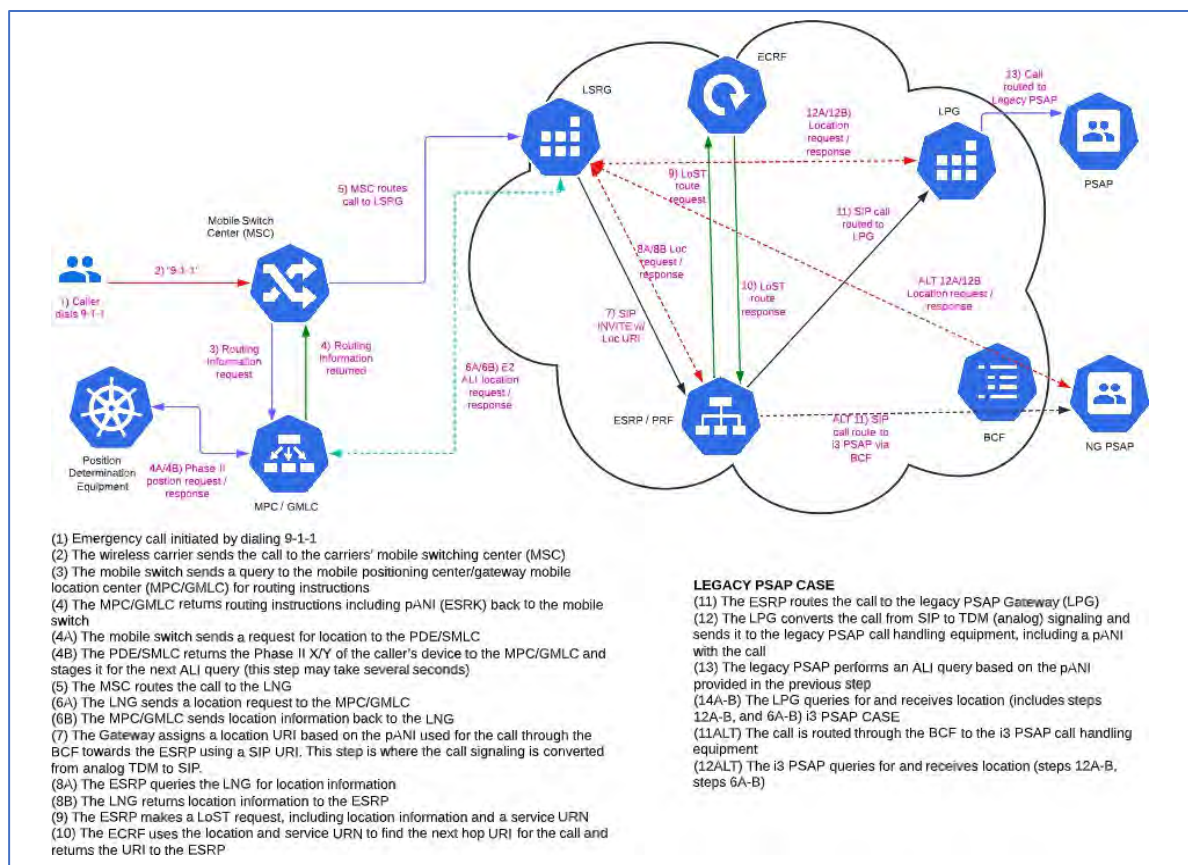


Figure 5-11: NENA Call Flow Scenario 2

Motorola Response

Understood

Section 6

Cost Sheet

Per the provided instructions, Motorola complies and has completed the cost sheet. Please see attachment 202691101 RFP Revised Cost Proposal Template Motorola File 2 of 4.

Section 7

Response to Terms

As a complete alternative to the State's proposed terms, Motorola proposes that the parties use its standard contract template as the controlling terms and conditions for Motorola's proposed offering to the State. Given the specifics of the Motorola service offering and the structures Motorola has put in place to for the services proposed to the State, Motorola believes its terms synchronize to that service offering more completely. That said, Motorola is always willing to engage in good faith negotiations with all of its customers regarding its terms and conditions. Thus, if selected and the State expresses any concerns with Motorola's terms or has specific terms it needs to be included, Motorola will be prepared to rapidly negotiate with the State on those terms and find mutually agreed language and other provisions to meet the State's needs.

Section 8

Contractual Agreement Form

As stated in Motorola's response to the Response to Terms, Motorola does take exception to the State's proposed terms as a whole, as Motorola proposes that its standard terms control over the offering, as may be changed through mutual negotiations with the State. As discussed there, Motorola has attached this agreement, as required by the State, and stands ready to negotiate any terms with the State.

CONTRACTUAL AGREEMENT FORM

BIDDER MUST COMPLETE THE FOLLOWING

By signing this Contractual Agreement Form, the bidder guarantees compliance with the provisions stated in this solicitation and agrees to the terms and conditions unless otherwise indicated in writing.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603, DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Vendors. This information is for statistical purposes only and will not be considered for contract award purposes.

X NEBRASKA VENDOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Vendor. "Nebraska Vendor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this Solicitation. All vendors who are not a Nebraska Vendor are considered Foreign Vendors under Neb. Rev Stat § 73-603 (c).

____ I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

____ I hereby certify that I am a blind person licensed by the Commission for the Blind & Visually Impaired in accordance with Neb. Rev. Stat. § 71-8611 and wish to have preference considered in the award of this contract.

FORM MUST BE SIGNED MANUALLY IN INK OR BY DOCUSIGN

BIDDER:	Motorola Solutions Connectivity, Inc.
COMPLETE ADDRESS:	500 W Monroe Ste 4400 St Chicago, IL 60661-3781
TELEPHONE NUMBER:	(936) 320-1035
FAX NUMBER:	NA
DATE:	April 15, 2026
SIGNATURE:	
TYPED NAME & TITLE OF SIGNER:	Travis Boettcher, CVP Software Sales

Motorola Solutions Connectivity Customer Agreement

This Motorola Solutions Customer Agreement (the “**MCA**”) is entered into between Motorola Solutions, Inc., and affiliated companies, with offices at 500 W. Monroe Street, Suite 4400, Chicago, IL 60661 (“**Motorola**”) and the entity purchasing Products (as defined below) from Motorola (“**Customer**”). Motorola and Customer will each be referred to herein as a “**Party**” and collectively as the “**Parties**”. This Agreement (as defined below) is effective as of the earlier of (a) the first purchase of a Product from Motorola, and (b) the date of the last signature on the Agreement (the “**Effective Date**”).

1. Agreement.

- 1.1. Scope; Agreement Documents. This MCA governs Customer’s purchase of Products (as defined below) from Motorola. Additional terms and conditions applicable to specific Products are set forth in one or more agreed upon addenda incorporated within this MCA (each an “**Addendum**”, and collectively the “**Addenda**”). This MCA, the applicable Addenda, and Proposal collectively form the Parties’ “**Agreement**”.
- 1.2. Order of Precedence. In interpreting this Agreement and resolving any ambiguities each Addendum will control with respect to conflicting terms in the Agreement, but only as applicable to the Products described in such Addendum. The Proposal will control with respect to conflicting terms in the MCA or any Addenda, but only as applicable to the Products and Services described in the Proposal.

2. Definitions.

“**Authorized Users**” means Customer’s employees and contractors engaged for the purpose of supporting or using the Products and Services on behalf of Customer, and that are not competitors of Motorola, and the entities (if any) specified in a Proposal or otherwise approved by Motorola in writing (email from an authorized Motorola signatory accepted), which may include affiliates or other Customer agencies.

“**Change Order**” means a written amendment to this Agreement after the Effective Date.

“**Communications System**” is a solution that includes at least one radio Product, whether devices, software, or infrastructure, and requires Integration Services to deploy such radio Product at a Customer Site or onto any Customer-Provided Equipment or Equipment provided to Customer.

“**Contract Price**” or “**Fees**” means the charges applicable to the Products, excluding applicable sales or similar taxes and freight charges.

“**Confidential Information**” means any and all non-public information provided by one Party to the other that is disclosed under this Agreement in oral, written, graphic, machine recognizable, or sample form, being clearly designated, labeled or marked as confidential or its equivalent or that a reasonable business person would consider non-public and confidential by its nature. With respect to Motorola, Confidential Information will also include Products, and Documentation, as well as any other information relating to the Products.

“**Customer Data**” has the meaning given to it in the DPA.

“**Customer-Provided Equipment**” means components, including equipment and software, not provided by Motorola which may be used with the Products.

“**Data Processing Addendum**” or “**DPA**” means the Motorola [Data Processing Addendum](#) applicable to processing of data, including Customer Data, as updated, supplemented, or superseded from time to time. The DPA is incorporated into and made a part of this Agreement for all purposes pertaining to the contents of the DPA. Where terms or provisions in the Agreement conflict with terms or provisions of the DPA, the terms or provisions of the DPA will control with respect to the contents of the DPA.

“**Delivery**” means the applicable delivery for a Product as described in Section 5.7 of this Agreement.

“Documentation” means the documentation for the Products, or data, that is delivered or made available with the Products that specifies technical and performance features, capabilities, users, or operation, including training manuals, and other deliverables, such as reports, specifications, designs, plans, drawings, analytics, or other information.

“Equipment” means hardware provided by Motorola.

“Equipment Lease-Purchase Agreement” means the agreement by which Customer finances all or a portion of the Contract Price.

“Feedback” means comments or information, in oral or written form, given to Motorola by Customer or Authorized Users, including end users, in connection with or relating to the Products.

“Integration Services” means the design, deployment, implementation, and integration Services provided by Motorola in order to design, install, set up, configure, and/or integrate the applicable Products as agreed upon by the Parties.

“Licensed Software” means software which is made available to Customer by Motorola (for example software preinstalled on Equipment, accessible via a website provided by Motorola, or software installed on or made available for Customer-Provided Equipment) and is licensed to Customer by Motorola.

“Lifecycle Management Services” or **“LMS”** means upgrade services as set out in the applicable Proposal.

“Maintenance and Support Services” means the break/fix maintenance, technical support, or other Services described in the applicable Proposal.

“Motorola Data” means data owned by Motorola and made available to Customer in connection with the Products;

“Motorola Materials” means proprietary equipment, hardware, content, software, tools, data, and other materials, including designs, utilities, models, methodologies, systems, and specifications, which Motorola has developed or licensed from third parties (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, or derivative works of the foregoing, whether made by Motorola or another party). Products, Motorola Data, Third-Party Data (as defined in the DPA), and Documentation, are considered Motorola Materials.

“Non-Motorola Materials” means collectively, Customer or third-party equipment, software, services, hardware, content, and data that is not provided by Motorola.

“Proposal” means solution descriptions, pricing, equipment lists, statements of work (**“SOW”**), schedules, technical specifications, quotes, order forms, and other documents setting forth the Products to be purchased by Customer and provided by Motorola. The Proposal may also include an Acceptance Test Plan (**“ATP”**); a **“Payment”** Form (Communications System purchase only); or a **“System Acceptance Certificate”** (Communications System only), depending on the Products purchased by Customer.

“Products” or **“Product”** is how the Equipment, Licensed Software and Services being purchased by the Customer is collectively referred to in this Agreement (collectively as **“Products”**, or individually as a **“Product”**).

“Professional Services” are services provided by Motorola to Customer under this Agreement, including Integration Services, the nature and scope of which are more fully described in the Proposal.

“Prohibited Jurisdiction” means any jurisdiction in which the provision of such Products is prohibited under applicable laws or regulations.

“Services” means services, including access to services, as described in the Proposal, and includes Integration Services, Subscription Services, Professional Services, Maintenance & Support Services, and Lifecycle Management Services provided by Motorola.

“Service Completion Date” means the date of Motorola’s completion of the Services described in a Proposal.

“Service Use Data” has the meaning given to it in the DPA.

“Site” or **“Sites”** means the location where the Integration Services, Lifecycle Management Services, or Maintenance and Support Services will take place.

“Software-as-a-Service” or **“SaaS”** means a solution that includes at least one Subscription Service and associated Licensed Software, which may include, as an example, client software or a web page.

“Software System” means a solution that includes at least one Licensed Software Product and requires Integration Services to deploy such Licensed Software Product at a Customer Site or onto any Customer-Provided Equipment or Equipment provided by or made available to Customer by Motorola.

“Subscription” means a recurring payment for Products, as set out in the Proposal.

“Subscription Services” or **“Recurring Services”** means Services, including access to Services, paid for on a subscription basis. Subscription Services includes services available through SaaS Products.

“Term” means the term of this MCA which will commence on the Effective Date and continue until six (6) months after the later of (a) the termination, expiration, or discontinuance of Services under the last Proposal in effect, or (b) the expiration of all applicable warranty periods, unless the MCA is earlier terminated as set forth herein.

3. Products and Services.

3.1. Products. Motorola will sell (a) Equipment, (b) licenses to Licensed Software, and (c) Services to Customer, to the extent each is set forth in this Agreement. At any time during the Term, Motorola may substitute any Products at no cost to Customer, if the substitute is substantially similar to the Products set forth in this Agreement. All Licensed Software is provided pursuant to the terms of the [Software License Agreement](#).

3.2. Services.

3.2.1. Motorola will provide Services, to the extent set forth in this Agreement.

3.2.2. Integration Services; Maintenance and Support Services. Motorola will provide (a) Integration Services at the applicable Sites, agreed upon by the Parties, or (b) Maintenance and Support Services or Lifecycle Management Services, each as further described in the applicable SOW. Terms applicable to Maintenance, Support and Lifecycle Management can be found in the [Maintenance, Support and Lifecycle Management Addendum](#).

3.2.3. Service Proposals. The Fees for Services will be set forth in Motorola’s Proposal. A Customer point of contact may be set forth in the applicable SOW for the Services.

3.2.4. Service Completion. Services described in a Proposal will be deemed complete upon the Service Completion Date, or as Services expire, or are renewed or terminated.

3.2.5. Professional Services

3.2.5.1. Additional Service Terms. If Customer is purchasing Professional Services to evaluate or assess networks, systems or operations; network security assessment or network monitoring; software application development Services; or transport connectivity services, [Additional Services Terms](#) apply.

3.3. Additional Product Terms. If the Products include one of the following Products or Product types, additional terms apply as found in the below links:
[AI Terms](#)
[Comparison Manager](#)

[Data licensed from Motorola](#)

[Drone related Products](#)

[Mobile Video Products, such as LPR cameras, bodycams, or vehicle cameras, and related software](#)

- 3.4. Non-Preclusion.** If, in connection with the Products provided under this Agreement, Motorola performs assessments of its own, or related, products or makes recommendations, including a recommendation to purchase other products, nothing in this Agreement precludes such efforts nor precludes Motorola from participating in a future competitive bidding process or otherwise offering or selling the recommended products to Customer. Customer represents that this paragraph does not violate its procurement standards or other laws, regulations, or policies.
- 3.5. Customer Obligations.** Customer represents that information Customer provides to Motorola in connection with receipt of Products are accurate and complete in all material respects. If any assumptions in the Proposals or information provided by Customer prove to be incorrect, or if Customer fails to perform any of its obligations under this Agreement, Motorola's ability to perform its obligations may be impacted and changes to the Agreement, including the scope, Fees, and performance schedule may be required.
- 3.6. Documentation.** Products may be delivered with Documentation. Documentation is and will be owned by Motorola, unless otherwise expressly stated in a Proposal that certain Documentation will be owned by Customer. Motorola hereby grants Customer a limited, royalty-free, worldwide, non-exclusive license to use the Documentation solely for its internal business purposes in connection with the Products.
- 3.7. Motorola Tools and Equipment.** As part of delivering the Products, Motorola may provide certain tools, equipment, models, and other materials of its own. Such tools and equipment will remain the sole property of Motorola unless they are to be purchased by Customer as Products and are explicitly listed on the Proposal. The tools and equipment may be held by Customer for Motorola's use without charge and may be removed from Customer's premises by Motorola at any time without restriction. Customer will safeguard all tools and equipment while in its custody or control, and be liable for any loss or damage. Upon the expiration or earlier termination of this Agreement, Customer, at its expense, will return to Motorola all such tools and equipment in its possession or control.
- 3.8. Authorized Users.** Customer will ensure its employees and Authorized Users comply with the terms of this Agreement and will be liable for all acts and omissions of its employees and Authorized Users. Customer is responsible for the secure management of Authorized Users' names, passwords and login credentials for access to Products.
- 3.9. Export Control.** Customer, its employees, and any other Authorized Users will not access or use the Products in any Prohibited Jurisdiction, and Customer will not provide access to the Products to any government, entity, or individual located in a Prohibited Jurisdiction. Customer represents and warrants that (a) it and its Authorized Users are not named on any U.S. government list of persons prohibited from receiving U.S. exports, or transacting with any U.S. person; (b) it and its Authorized Users are not a national of, or a company registered in, any Prohibited Jurisdiction; (c) Customer will not permit its Authorized Users to access or use the Products or Services in violation of any U.S. or other applicable export embargoes, prohibitions or restrictions; and (d) Customer and its Authorized Users will comply with all applicable laws regarding the transmission of technical data exported from the U.S. and the country in which Customer, its employees, and the Authorized Users are located.
- 3.10. Change Orders.** Unless a different change control process is agreed upon in writing by the Parties, a Party may request changes to an Addendum or a Proposal by submitting a Change Order to the other Party. If a requested change causes an increase or decrease in the Products, the Parties by means of the Change Order will make appropriate adjustments to the Fees, project schedule, or other matters. Change Orders are effective and binding on the Parties only upon execution of the Change Order by an authorized representative of both Parties.

4. Term and Termination.

- 4.1. Term.** The applicable Addendum or Proposal will set forth the Term for the Products governed thereby.

- 4.1.1. Subscription Terms.** Unless otherwise specified in the Proposal, if the Products are purchased as a Subscription, the Subscription commences upon Delivery of, or Customer having access to, the first applicable Product ordered under this Agreement and will continue for a twelve (12) month period or such other period identified in a Proposal (the “**Initial Subscription Period**”) and, unless otherwise stated in the Proposal, will automatically renew for additional twelve (12) month periods (each, a “**Renewal Subscription Year**”), unless either Party notifies the other of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. (The Initial Subscription Period and each Renewal Subscription Year will each be referred to herein as a “**Subscription Term**”.) Motorola may increase Fees prior to any Renewal Subscription Year by notifying Customer of the proposed increase no later than thirty (30) days prior to commencement of the Renewal Subscription Year.
- 4.2. Termination.** Either Party may terminate the Agreement or the applicable Addendum or Proposal if the other Party breaches a material obligation under the Agreement and does not cure such breach within thirty (30) days after receipt of notice of the breach or fails to produce a cure plan within such period of time. Each Addendum and Proposal may be separately terminable as set forth therein.
- 4.3. Termination for Non-Appropriation.** In the event any identified funding is not appropriated or becomes unavailable, the Customer reserves the right to terminate this Agreement for non-appropriation upon thirty (30) days’ advance written notice to Motorola. In the event of such termination, Motorola shall be entitled to compensation for all conforming Products delivered or performed prior to the date of termination.
- 4.4. Suspension of Services.** Motorola may promptly terminate or suspend any Products under a Proposal if Motorola determines: (a) the related Product license has expired or has terminated for any reason; (b) the applicable Product is being used on a hardware platform, operating system, or version not approved by Motorola; (c) Customer fails to make any payments when due; or (d) Customer fails to comply with any of its other obligations or otherwise delays Motorola’s ability to perform.
- 4.5. Wind Down of Subscription.** In addition to the termination rights in this Agreement, Motorola may terminate any Subscription Term, in whole or in part, in the event Motorola plans to cease offering the applicable Licensed Software or Subscription Services to customers.
- 4.6. Effect of Termination or Expiration.** Upon termination for any reason or expiration of this Agreement, an Addendum, or a Proposal, Customer and the Authorized Users will return or destroy (at Motorola’s option) all Motorola Materials and Motorola’s Confidential Information in their possession or control and, as applicable, provide proof of such destruction, except that Equipment purchased by Customer should not be returned. If Customer has any outstanding payment obligations under this Agreement, Motorola may accelerate and declare all such obligations of Customer immediately due and payable by Customer. Notwithstanding the reason for termination or expiration, Customer agrees to pay Motorola for Products already delivered or performed. Customer has a duty to mitigate any damages under this Agreement, including in the event of default by Motorola and Customer’s termination of this Agreement.
- 4.7. Equipment.** In the event that Customer purchases any Product at a price below the published list price for such Product in connection with Customer entering into a fixed- or minimum required-term agreement for Products, and Customer or Motorola terminates the Agreement prior to the expiration of such fixed- or minimum required-term, then Motorola will have the right to invoice Customer for, and Customer will pay, the amount of the discount to the published list price for the Product or such other amount set forth in writing. This Section will not limit any other remedies Motorola may have with respect to an early termination.
- 5. Payment, Invoicing, Delivery and Risk of Loss**
- 5.1.** The Contract Price of \$_____, excluding taxes, is fully committed and identified, including all subsequent years of any contracted Services. The Customer will pay all invoices as received from Motorola subject to the terms of this Agreement and any changes in scope will be subject to the change order process as described in this Agreement.

Motorola acknowledges the Customer may require the issuance(s) of a purchase order or notice to proceed as part of the Customer's procurement process. However, Customer agrees that the issuance or non-issuance of a purchase order or notice to proceed does not preclude the Customer from its contractual obligations as defined in this Agreement.

- 5.2. Fees.** Fees and charges applicable to the Products will be as set forth in the applicable Proposal. Changes in the scope of Products described in a Proposal that require an adjustment to the Fees will be set forth in the applicable pricing schedule. The Fees for any Products exclude expenses associated with unusual and costly Site access requirements (e.g., if Site access requires a helicopter or other equipment), tariffs, fluctuations in the costs of energy, raw materials, and fuel. Motorola reserves the right to equitably adjust the Fees for these expenses upon written notice to Customer. Customer will reimburse Motorola for expenses reasonably incurred by Motorola in connection with the Products. The annual Subscription Fee for Products may include certain one-time Fees, such as start-up fees, license fees, or other fees set forth in a Proposal. Motorola may suspend Licensed Software and any Subscription Services if Customer fails to make any payments within thirty (30) days of invoice due date when due.
- 5.3. Taxes.** The Fees do not include any excise, sales, lease, use, property, or other taxes, assessments, duties, or regulatory charges or contribution requirements (collectively, "**Taxes**"), all of which will be paid by Customer, except as exempt by law, unless otherwise specified in a Proposal. If Motorola is required to pay any Taxes, Customer will reimburse Motorola for such Taxes (including any interest and penalties) within thirty (30) days after Customer's receipt of an invoice therefore. Customer will be solely responsible for reporting the Products for personal property tax purposes, and Motorola will be solely responsible for reporting taxes on its income and net worth.
- 5.4. Invoicing.** Motorola will invoice Customer as described in this Agreement and Customer will pay all invoices within thirty (30) days of the invoice date or as otherwise specified in writing. In the event Customer finances the purchase of the Motorola Products contemplated herein via Motorola Solutions Credit Corporation ("MSCC"), invoices for such purchase will be paid via the disbursement of the financing proceeds pursuant to the Equipment Lease - Purchase Agreement executed between the parties and the payment schedule enclosed therein shall control payment of the related invoices. Late payments will be subject to interest charges at the maximum rate permitted by law, commencing upon the due date. Motorola may invoice electronically via email, and Customer agrees to receive invoices via email at the email address set forth in Section 5.6. Customer acknowledges and agrees that a purchase order or other notice to proceed is not required for payment for Products.
- 5.5. Payment.** Customer will pay invoices for the Products provided under this Agreement in accordance with the invoice payment terms set forth in Section 5.4. Generally, invoices are issued after shipment of Equipment or upon Motorola's Delivery of Licensed Software, Customer access to SaaS, or upon System Completion Date of a Software System, as applicable, but if a specific invoicing or payment schedule is set forth in the Agreement, such schedule will determine the invoicing cadence.

Motorola will have the right to suspend future Deliveries of Products if Customer fails to make any payments when due.

- 5.6. INVOICING AND SHIPPING ADDRESSES.** Invoices will be sent to the Customer at the following address:

Name: _____
Address: _____
Phone: _____

E-INVOICE. To receive invoices via email:

Customer Account Number: _____
Customer Accounts Payable Email: _____
Customer CC (optional) Email: _____

The address which is the ultimate destination where the Equipment will be delivered to Customer is:

Name: _____

Address: _____

The Equipment will be shipped to the Customer at the following address (insert if this information is known):

Name: _____

Address: _____

Phone: _____

Customer may change this information by giving written notice to Motorola.

- 5.7. Delivery, Title and Risk of Loss.** Motorola will provide to Customer the Products set forth in a Proposal, in accordance with the terms of the Agreement. Motorola will, using commercially reasonable practices, pack the ordered Equipment and ship such Equipment to the Customer address set forth in **Section 5.6** or otherwise provided by Customer in writing, using a carrier selected by Motorola.

Notwithstanding the foregoing and unless otherwise stated in a Equipment Lease - Purchase Agreement, Delivery of Equipment (and any incorporated Licensed Software) will occur, and title and risk of loss for the Equipment will pass to Customer, upon shipment by Motorola in accordance with ExWorks, Motorola's premises (Incoterms 2020). Customer will pay all shipping costs, taxes, and other charges applicable to the shipment and import or export of the Products and Services, as applicable, and Customer will be responsible for reporting the Products for personal property tax purposes.

Delivery of Licensed Software for installation on Equipment or Customer-Provided Equipment will occur upon the earlier of (a) electronic delivery of the Licensed Software by Motorola, or (b) the date Motorola otherwise makes the Licensed Software available for download or use by Customer. If agreed upon in a Proposal, Motorola will also provide Services related to such Products. Title to Licensed Software will not pass to Customer at any time. Delivery of SaaS Products will occur when the Services are made available to Customer.

- 5.8. Delays.** Any shipping dates set forth in a Proposal are approximate. While Motorola will make reasonable efforts to ship Products by any such estimated shipping date, Motorola will not be liable for any delay or related damages to Customer. Time for Delivery will not be of the essence, and delays will not constitute grounds for cancellation, penalties, termination, or a refund.
- 5.9. Future Regulatory Requirements.** The Parties acknowledge and agree that certain Products (for example, cyber services) are in evolving technological areas and therefore, laws and regulations regarding Products may change. Changes to existing Products required to achieve regulatory compliance may be available for an additional fee. Any required changes may also impact the price for Products.
- 5.10. Resale of Equipment.** Equipment may contain embedded Licensed Software. If Customer desires to sell its used Equipment to a third party, Customer must first receive prior written authorization from Motorola, which will not be unreasonably denied, and obtain written acceptance of the applicable Licensed Software license terms, including the obligation to pay relevant license fees, from such third party. Customer will take appropriate security measures when disposing of Equipment, including the deletion of all data stored in the Equipment.

6. Sites; Customer-Provided Equipment; Non-Motorola Materials.

- 6.1. Access to Sites.** Customer will be responsible for providing all necessary permits, licenses, and other approvals necessary for the performance, installation and use of the Products at each applicable Site, including for Motorola to perform its obligations hereunder, and for facilitating Motorola's access to the Sites. No waivers of liability will be imposed on Motorola or its subcontractors by Customer or others at Customer facilities or other Sites, but if and to the extent any such waivers are imposed, the Parties agree such waivers are void.

- 6.2. Site Conditions.** Customer will ensure that (a) all Sites are safe and secure, (b) Site conditions meet all applicable industry and legal standards (including standards promulgated by OSHA or other governmental or regulatory bodies), (c) to the extent applicable, Sites have adequate physical space, air conditioning, and other environmental conditions, electrical power outlets, distribution, equipment, connections, and telephone or other communication lines (including modem access and interfacing networking capabilities), and (d) Sites are suitable for the installation, use, and maintenance of the Products. This Agreement is predicated upon normal soil conditions as defined by the version of E.I.A. standard RS-222 in effect on the Effective Date.
- 6.3. Site Issues.** Upon its request, which will not be unreasonably denied, Motorola will have the right to inspect the Sites and advise Customer of any deficiencies or non-conformities with the requirements of this **Section 6 – Sites; Customer-Provided Equipment; Non-Motorola Materials**. If Motorola or Customer identifies any deficiencies or non-conformities, Customer will promptly remediate such issues or the Parties will select a replacement Site. If a Party determines that a Site identified in a Proposal is not acceptable or desired, the Parties will cooperate to investigate the conditions and select a replacement Site or otherwise adjust the installation plans and specifications as necessary. A change in Site or adjustment to the installation plans and specifications may cause a change in the Fees or performance schedule under the applicable Proposal.
- 6.4. Customer-Provided Equipment.** Customer will be responsible, at its sole cost and expense, for providing and maintaining the Customer-Provided Equipment in good working order. Customer represents and warrants that it has all rights in Customer-Provided Equipment to permit Motorola to access and use the applicable Customer-Provided Equipment to provide the Products under this Agreement, and such access and use will not violate any laws or infringe any third-party rights (including intellectual property rights). Customer (and not Motorola) will be fully liable for Customer-Provided Equipment, and Customer will immediately notify Motorola of any Customer-Provided Equipment damage, loss, change, or theft that may impact Motorola's ability to provide the Products under this Agreement, and Customer acknowledges that any such events may cause a change in the Fees or performance schedule under the applicable Proposal.
- 6.5. Non-Motorola Materials.** In certain instances, Customer may be permitted to access, use, or integrate Non-Motorola Materials with or through the Products. If Customer accesses, uses, or integrates any Non-Motorola Materials with the Products, Customer will first obtain all necessary rights and licenses to permit Customer's and its Authorized Users' use of the Non-Motorola Materials in connection with the Products. Customer will also obtain the necessary rights for Motorola to use such Non-Motorola Materials in connection with providing the Products, including the right for Motorola to access, store, and process such Non-Motorola Materials (e.g., in connection with SaaS Products), and to otherwise enable interoperation with the Products. Customer represents and warrants that it will obtain the foregoing rights and licenses prior to accessing, using, or integrating the applicable Non-Motorola Materials with the Products, and that Customer and its Authorized Users will comply with any terms and conditions applicable to such Non-Motorola Materials. If any Non-Motorola Materials requires access to Customer Data, Customer hereby authorizes Motorola to allow the provider of such Non-Motorola Materials to access Customer Data, in connection with the interoperation of such Non-Motorola Materials with the Products.
- 6.6.** Customer acknowledges and agrees that Motorola is not responsible for, and makes no representations or warranties with respect to, the Non-Motorola Materials (including any disclosure, modification, or deletion of Customer Data resulting from use of Non-Motorola Materials or failure to properly interoperate with the Products). If Customer receives notice that any Non-Motorola Materials must be removed, modified, or disabled within the Products, Customer will promptly do so. Motorola will have the right to disable or remove Non-Motorola Materials if Motorola believes a violation of law, third-party rights, or Motorola's policies is likely to occur, or if such Non-Motorola Materials poses or may pose a security or other risk or adverse impact to the Products, Motorola, Motorola's systems, or any third party (including other Motorola customers).
- 6.7.** Motorola may provide certain Non-Motorola Materials as an authorized sales representative of a third party as set out in a Proposal. As an authorized sales representative, the third party's [terms and conditions](#) will apply to any such sales. Any orders for such Non-Motorola Materials will be fulfilled by the third party.

- 6.8. End User Licenses.** Notwithstanding any provision to the contrary in the Agreement, certain Non-Motorola Materials software are governed by a separate license, EULA, or other agreement, including terms governing third-party equipment or software, such as open source software, included in the Products. Customer will comply, and ensure its Authorized Users comply, with any such additional terms applicable to third-party equipment or software. Certain [third party flow-down terms](#) applicable to Motorola Products may apply.
- 6.9. Prohibited Use.** Customer will not integrate or use, or permit a third party or an Authorized User to integrate or use, any Non-Motorola Materials with or in connection with a Software System or other Licensed Software provided by Motorola under this Agreement, without the express written permission of Motorola.
- 6.10. API and Client Support.** Motorola will use reasonable efforts to maintain its Application Programming Interfaces (APIs) for each Software System, understanding that APIs will evolve. Motorola will support each API version for 6 months after introduction but may discontinue support with reasonable notice or without notice if a security risk is present. For Licensed Software requiring a local client installation, Customer is responsible for installing the current version. Motorola will support each client version for 45 days after its release but may update the client at any time, and does not guarantee support for prior client versions.

7. Representations and Warranties.

- 7.1. Mutual Representations and Warranties.** Each Party represents and warrants to the other Party that (a) it has the right to enter into, and execute, the Agreement and perform its obligations hereunder, and (b) the Agreement will be binding on such Party.
- 7.2. System Warranty.** Subject to the disclaimers and exclusions below, Motorola represents and warrants that, on the date of System Acceptance (for Communications Systems), System Completion Date (for Software Systems), or Delivery, as applicable (a) the Communications System will perform in accordance with the descriptions in the applicable Proposal in all material respects, (b) the Software System will perform in accordance with the descriptions in the applicable Proposals in all material respects, and (c) if Customer has purchased any Licensed Software (but, for clarity, excluding SaaS Products) as part of such Communications System or Software System, the warranty period applicable to such Licensed Software will continue for a period of one (1) year commencing upon System Acceptance, System Completion, or date the Licensed Software is delivered (the "**Warranty Period**").
- 7.3. Communications Systems.** During the Warranty Period, in addition to warranty services, Motorola will provide Maintenance and Support Services for the Equipment and support for the Motorola Licensed Software in Communication Systems pursuant to the applicable maintenance and support Proposal. Support for the Licensed Software will be in accordance with Motorola's established [Software Support Policy](#) ("SwSP"). If Customer wishes to purchase (a) additional Maintenance and Support Services during the Warranty Period; or (b) continue or expand maintenance, software support, installation, and/or Motorola's LMS after the Warranty Period, Motorola will provide the description of and pricing for such services in a separate proposal document and such terms will be agreed upon in a Proposal. Unless otherwise agreed by the Parties in writing, the terms and conditions of the MSLMA referenced in Section 3.2.2 will govern the provision of such Services.
- 7.4. SaaS.** SaaS Products do not qualify for the System Warranty above.
- 7.5. Motorola Warranties - Services.** Subject to the disclaimers and exclusions below, Motorola represents and warrants that (a) Services will be provided in a good and workmanlike manner and will conform in all material respects to the descriptions in the applicable Proposal; and (b) for a period of ninety (90) days commencing upon the Service Completion Date for one-time Services, the Services will be free of material defects in materials and workmanship. Other than as set forth in subsection (a) above, recurring Services are not warranted but rather will be subject to the requirements of the applicable Addendum or Proposal.

- 7.6. Motorola Warranties - Equipment. Subject to the disclaimers and exclusions set forth below, (a) for a period of one (1) year commencing upon the Delivery of Motorola-manufactured Equipment under **Section 5.7 – Delivery, Title and Risk of Loss**, Motorola represents and warrants that such Motorola-manufactured Equipment, under normal use, will be free from material defects in materials and workmanship; and (b) the warranties applicable to Motorola-manufactured Equipment set forth in herein shall be applicable to all radio Equipment purchased hereunder whether or not such Equipment was manufactured by Motorola.
- 7.7. Warranty Claims; Remedies. To assert a warranty claim, Customer must notify Motorola in writing of the claim prior to the expiration of any warranty period set forth in this Agreement. Unless a different remedy is otherwise expressly set forth herein, upon receipt of such claim, Motorola will investigate the claim and use commercially reasonable efforts to repair or replace any confirmed materially non-conforming Product or re-perform any non-conforming Service, at its option. Such remedies are Customer's sole and exclusive remedies for Motorola's breach of a warranty. Motorola's warranties are extended by Motorola to Customer only, and are not assignable or transferable.
- 7.8. Pass-Through Warranties. Notwithstanding any provision of this Agreement to the contrary, Motorola will have no liability for third-party software or hardware provided by Motorola; provided, however, that to the extent offered by third-party providers of software or hardware and to the extent permitted by law, Motorola will pass through express warranties provided by such third parties.
- 7.9. WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS AND PASS THROUGH WARRANTIES IN THIS AGREEMENT, PRODUCTS AND SERVICES PURCHASED HEREUNDER ARE PROVIDED "AS IS" AND WITH ALL FAULTS. WARRANTIES SET FORTH IN THE AGREEMENT ARE THE COMPLETE WARRANTIES FOR THE PRODUCTS AND SERVICES AND MOTOROLA DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND QUALITY. MOTOROLA DOES NOT REPRESENT OR WARRANT THAT USE OF THE PRODUCTS AND SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE OF SECURITY VULNERABILITIES, OR THAT THEY WILL MEET CUSTOMER'S PARTICULAR REQUIREMENTS.
- 7.10. ADDITIONAL WARRANTY EXCLUSIONS. NOTWITHSTANDING ANY PROVISION OF THE AGREEMENT TO THE CONTRARY, MOTOROLA WILL HAVE NO LIABILITY FOR (A) DEFECTS IN OR DAMAGE TO PRODUCTS RESULTING FROM USE OTHER THAN IN THE NORMAL AUTHORIZED MANNER, OR FROM ACCIDENT, LIQUIDS, OR NEGLIGENCE; (B) TESTING, MAINTENANCE, REPAIR, INSTALLATION, OR MODIFICATION BY PARTIES OTHER THAN MOTOROLA; (C) CUSTOMER'S OR ANY AUTHORIZED USER'S FAILURE TO COMPLY WITH INDUSTRY AND OSHA OR OTHER LEGAL STANDARDS; (D) DAMAGE TO RADIO ANTENNAS, UNLESS CAUSED BY DEFECTS IN MATERIAL OR WORKMANSHIP; (E) EQUIPMENT WITH NO SERIAL NUMBER; (F) BATTERIES OR CONSUMABLES; (G) FREIGHT COSTS FOR SHIPMENT TO REPAIR DEPOTS; (H) COSMETIC DAMAGE THAT DOES NOT AFFECT OPERATION; (I) NORMAL WEAR AND TEAR; (J) ISSUES OR OBSOLESCENCE OF LICENSED SOFTWARE DUE TO CHANGES IN CUSTOMER OR AUTHORIZED USER REQUIREMENTS, EQUIPMENT, OR SYSTEMS; (K) TRACKING AND LOCATION-BASED SERVICES; OR (L) BETA SERVICES.
8. **Indemnification.**
- 8.1. General Indemnity. Motorola will defend, indemnify, and hold Customer harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual third-party claim, demand, action, or proceeding ("Claim") for personal injury, death, or direct damage to tangible property to the extent caused by Motorola's negligence, gross negligence or willful misconduct while performing its duties under this Agreement, except to the extent the claim arises from Customer's negligence or willful misconduct. Motorola's duties under this **Section 8.1 – General Indemnity** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise to the extent allowed by applicable law; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Claim.

8.2. Intellectual Property Infringement. Motorola will defend Customer against any third-party claim alleging that a Motorola-developed or manufactured Product (the "Infringing Product") directly infringes a United States patent or copyright ("Infringement Claim"), and Motorola will pay all damages finally awarded against Customer by a court of competent jurisdiction for an Infringement Claim, or agreed to in writing by Motorola in settlement of an Infringement Claim. Motorola's duties under this **Section 8.2 – Intellectual Property Infringement** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Infringement Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Infringement Claim.

8.2.1. If an Infringement Claim occurs, or in Motorola's opinion is likely to occur, Motorola may at its option and expense: (a) procure for Customer the right to continue using the Infringing Product; (b) replace or modify the Infringing Product so that it becomes non-infringing; or (c) grant Customer (i) a prorated refund of any amounts pre-paid for the Infringing Product (if the Infringing Product is Licensed Software) or (ii) a credit for the Infringing Product, less a reasonable charge for depreciation (if the Infringing Product is Equipment, including Equipment with embedded Licensed Software).

8.2.2. In addition to the other damages disclaimed under this Agreement, Motorola will have no duty to defend or indemnify Customer for any Infringement Claim that arises from or is based upon: (a) Customer Data, Customer-Provided Equipment, Non-Motorola Materials, or third-party equipment, hardware, software, data, or other third-party materials; (b) the combination of the Product with any products or materials not provided by Motorola; (c) a Product designed, modified, or manufactured in accordance with Customer's designs, specifications, guidelines or instructions; (d) a modification of the Product by a party other than Motorola; (e) use of the Product in a manner for which the Product was not designed or that is inconsistent with the terms of this Agreement; or (f) the failure by Customer to use or install an update to the Product that is intended to correct the claimed infringement. In no event will Motorola's liability resulting from an Infringement Claim extend in any way to any payments due on a royalty basis, other than a reasonable royalty based upon revenue derived by Motorola from Customer from sales or license of the Infringing Product.

8.2.3. This **Section 8.2 – Intellectual Property Infringement** provides Customer's sole and exclusive remedies and Motorola's entire liability in the event of an Infringement Claim.

8.3. Customer Indemnity. To the extent allowed by applicable law, Customer will defend, indemnify, and hold Motorola and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to (a) Customer-Provided Equipment, Customer Data, or Non-Motorola Materials, including any claim, demand, action, or proceeding alleging that any such equipment, data, or materials (or the integration or use thereof with the Products) infringes or misappropriates a third-party intellectual property or other right, violates applicable law, or breaches the Agreement; (b) Customer-Provided Equipment's failure to meet the minimum requirements set forth in the applicable Documentation or match the applicable specifications provided to Motorola by Customer in connection with the Products; (c) Customer's (or its service providers, agents, employees, or Authorized User's) negligence or willful misconduct; and (d) Customer's or its Authorized User's breach of this Agreement. This indemnity will not apply to the extent any such claim is caused by Motorola's use of Customer-Provided Equipment, Customer Data, or Non-Motorola Materials in violation of the Agreement. Motorola will give Customer prompt, written notice of any claim subject to the foregoing indemnity. Motorola will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

9. Limitation of Liability.

9.1. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF MOTOROLA, ITS AFFILIATES, AND ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, AGENTS, SUCCESSORS, AND ASSIGNS (COLLECTIVELY, THE "MOTOROLA PARTIES"), WHETHER BASED ON A CLAIM IN CONTRACT OR IN TORT, LAW OR EQUITY, RELATING TO OR ARISING OUT OF THE AGREEMENT WILL NOT EXCEED THE FEES, OR PORTION OF FEES,

RELATED TO THE PRODUCT UNDER WHICH THE CLAIM AROSE. WITH RESPECT TO ANY RECURRING SERVICES, THE MOTOROLA PARTIES' TOTAL AGGREGATE LIABILITY FOR ALL CLAIMS RELATED TO SUCH RECURRING SERVICES WILL NOT EXCEED THE TOTAL FEES PAID FOR THE APPLICABLE PRODUCT DURING THE CONSECUTIVE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT FROM WHICH THE FIRST CLAIM AROSE. EXCEPT FOR PERSONAL INJURY OR DEATH, THE MOTOROLA PARTIES WILL NOT BE LIABLE IN CONNECTION WITH THIS AGREEMENT (WHETHER UNDER MOTOROLA'S INDEMNITY OBLIGATIONS, A CAUSE OF ACTION FOR BREACH OF CONTRACT, UNDER TORT THEORY, OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF MOTOROLA HAS BEEN ADVISED BY CUSTOMER OR ANY THIRD PARTY OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES AND WHETHER OR NOT SUCH DAMAGES OR LOSSES ARE FORESEEABLE.

- 9.2. EXCLUSIONS FROM LIABILITY.** NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, MOTOROLA WILL HAVE NO LIABILITY FOR DAMAGES ARISING OUT OF (A) CUSTOMER DATA, INCLUDING ITS TRANSMISSION TO MOTOROLA, OR ANY OTHER DATA AVAILABLE THROUGH THE PRODUCTS; (B) CUSTOMER-PROVIDED EQUIPMENT OR SITES; NON-MOTOROLA MATERIALS; THIRD-PARTY EQUIPMENT, HARDWARE, SOFTWARE, DATA, OR CONTENT; OR UNKNOWN OR UNAUTHORIZED COMBINATION OF PRODUCTS AND SERVICES; (C) LOSS OF DATA, HACKING, RANSOMWARE, THIRD-PARTY ATTACKS OR DEMANDS; (D) MODIFICATION OF PRODUCTS NOT AUTHORIZED BY MOTOROLA; (E) RECOMMENDATIONS PROVIDED IN CONNECTION WITH THE PRODUCTS PROVIDED UNDER THIS AGREEMENT; (F) DATA RECOVERY SERVICES OR DATABASE MODIFICATIONS; OR (G) CUSTOMER'S OR ANY AUTHORIZED USER'S BREACH OF THIS AGREEMENT OR MISUSE OF THE PRODUCTS.

IN ADDITION TO THE FOREGOING EXCLUSIONS FROM DAMAGES, AND NOTWITHSTANDING ANY PROVISION OF THE AGREEMENT TO THE CONTRARY, MOTOROLA WILL HAVE NO LIABILITY FOR (A) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS; (B) DISRUPTION OF OR DAMAGE TO CUSTOMER'S OR THIRD PARTIES' SYSTEMS, EQUIPMENT, OR DATA, INCLUDING DENIAL OF ACCESS TO USERS, OR SHUTDOWN OF SYSTEMS CAUSED BY INTRUSION DETECTION SOFTWARE OR HARDWARE; (C) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH SOFTWARE-AS-A-SERVICE, OR INTERPRETATION, USE, OR MISUSE THEREOF; (D) TRACKING AND LOCATION-BASED SERVICES; OR (E) BETA SERVICES.

- 9.3. Statute of Limitations.** Customer may not bring any claims against a Motorola Party in connection with this Agreement or the Products and Services more than one (1) year after the date of accrual of the cause of action.

10. Confidentiality.

- 10.1. Confidential Information.** Customer and Motorola agree that, subject to any applicable freedom of information or public records legislation, Motorola's [Confidentiality Terms](#) apply to information shared between the Parties.

11. Proprietary Rights; Data; Feedback.

- 11.1. Motorola Materials.** Customer acknowledges that Motorola may use or provide Customer with access to "Motorola Materials". Except when Motorola has expressly transferred title or other interest to Customer in writing, the Motorola Materials are the property of Motorola or its licensors, and Motorola or its licensors retain all right, title and interest in and to the Motorola Materials (including, all rights in patents, copyrights, trademarks, trade names, trade secrets, know-how, other intellectual property and proprietary rights, and all associated goodwill and moral rights).

This Agreement does not grant to Customer any shared development rights in or to any Motorola Materials or other intellectual property, and Customer agrees to execute any documents and take any other actions reasonably requested by Motorola to effectuate the foregoing. Motorola and its licensors reserve all rights not expressly granted to Customer, and no rights, other than those expressly granted herein, are granted

to Customer by implication, estoppel or otherwise. Customer will not modify, disassemble, reverse engineer, derive source code or create derivative works from, merge with other software, distribute, sublicense, sell, or export the Products and Services or other Motorola Materials, or permit any third party to do so.

- 11.2. Ownership of Customer Data.** Customer retains all right, title and interest, including intellectual property rights, if any, in and to Customer Data. Motorola acquires no rights to Customer Data except those rights granted under this Agreement including the right to Process (as defined in the DPA) and use the Customer Data as set forth in the DPA.
- 11.3. Feedback.** Any Feedback provided by Customer is entirely voluntary, and will not create any confidentiality obligation for Motorola, even if designated as confidential by Customer. Motorola may use, reproduce, license, and otherwise distribute and exploit the Feedback without any obligation or payment to Customer or Authorized Users and Customer represents and warrants that it has obtained all necessary rights and consents to grant Motorola the foregoing rights.
- 11.4. Improvements: Products and Services.** The Parties agree that, notwithstanding any provision of this Agreement to the contrary, all fixes, modifications and improvements to the Services or Products conceived of or made by or on behalf of Motorola that are based either in whole or in part on the Feedback, Customer Data, or Service Use Data (or otherwise) are the exclusive property of Motorola and all right, title and interest in and to such fixes, modifications or improvements will vest solely in Motorola. Customer agrees to execute any written documents necessary to assign any intellectual property or other rights it may have in such fixes, modifications or improvements to Motorola.

12. Acceptance

- 12.1. Communications System Acceptance.** Unless further defined in the applicable Proposal or Statement of Work, System Acceptance for a Communications System occurs upon successful completion of Acceptance Tests as detailed in the Acceptance Test Plan. Motorola will provide ten days' notice before testing begins, and upon successful completion, both parties will sign an acceptance certificate. If the plan includes tests for subsystems or phases, acceptance occurs upon successful completion of those tests and separate certificates will be issued. If Customer believes the system has failed, they must provide a detailed written notice within thirty days; otherwise, System Acceptance is deemed to have occurred. Minor, non-material issues will not delay acceptance but will be addressed per a mutually agreed schedule. Customer use of the system before System Acceptance requires Motorola's written authorization and transfers responsibility for system operation to the Customer. Software System Completion is defined by Customer's Beneficial Use of each Product within the system, with "Beneficial Use" defined to occur thirty days after functional demonstration if not otherwise defined in the Proposal.

13. Force Majeure; Delays Caused by Customer.

- 13.1. Force Majeure.** Except for Customer's payment obligations hereunder, neither Party will be responsible for nonperformance or delayed performance due to events outside of its reasonable control. If performance will be significantly delayed, the affected Party will provide notice to the other Party, and the Parties will agree (in writing) upon a reasonable extension to any applicable performance schedule.
- 13.2. Delays Caused by Customer.** Motorola's performance of the Products will be excused for delays caused by Customer or its Authorized Users or subcontractors, or by failure of any assumptions set forth in this Agreement (including in any Addendum or Proposal). In the event of a delay under this **Section 13.2 – Delays Caused by Customer**, (a) Customer will continue to pay the Fees as required hereunder, (b) the Parties will agree (in writing) upon a reasonable extension to any applicable performance schedule, and (c) Customer will compensate Motorola for its out-of-pocket costs incurred due to the delay (including those incurred by Motorola's affiliates, vendors, and subcontractors).

- 14. Disputes.** The Parties will use the following procedure to resolve any disputes relating to or arising out of this Agreement (each, a "Dispute"):

- 14.1. Governing Law.** All matters relating to or arising out of the Agreement are governed by the laws of the State of Illinois, unless Customer is the United States Government (or an agency thereof) or a state government or state agency or local municipality within the United States, in which case all matters relating to or arising out of the Agreement will be governed by the laws of the State in which the Products and Services are provided. The terms of the U.N. Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act will not apply.
- 14.2. Negotiation; Mediation.** The Parties will attempt to timely resolve the Dispute promptly through good faith negotiations. Either Party may initiate dispute resolution procedures by sending a notice of Dispute ("Notice of Dispute") to the other Party. The Parties will choose an independent mediator within thirty (30) days of such Notice of Mediation. Neither Party may unreasonably withhold consent to the selection of a mediator, but if the Parties are unable to agree upon a mediator, either Party may request that the American Arbitration Association nominate a mediator. Each Party will bear its own costs of mediation, but the Parties will share the cost of the mediator equally. Unless otherwise agreed in writing, all in person meetings under this **Section 14.2 – Negotiation; Mediation** will take place in Chicago, Illinois, and all communication relating to the Dispute resolution will be maintained in strict confidence by the Parties. Notwithstanding the foregoing, any Dispute arising from or relating to Motorola's intellectual property rights must be decided by a court of competent jurisdiction, in accordance with **Section 14.3 – Litigation, Venue, Jurisdiction** below.
- 14.3. Litigation, Venue, Jurisdiction.** If the Dispute has not been resolved by mediation within sixty (60) days from the Notice of Mediation, either Party may submit the Dispute exclusively to a court in Cook County, Illinois, or in the case the Customer is the United States, a state agency, or local municipality, then the appropriate court in the State in which the Products and Services are provided. Each Party expressly consents to the exclusive jurisdiction of such courts for resolution of any Dispute and to enforce the outcome of any mediation.
- 15. General.**
- 15.1. Compliance with Laws.** Each Party will comply with applicable laws in connection with the performance of its obligations under this Agreement, including that Customer will ensure its and its Authorized Users' use of the Products complies with law (including privacy laws), and Customer will obtain any FCC, FAA, and other licenses or authorizations (including licenses or authorizations required by foreign regulatory bodies) required for its and its Authorized Users' use of the Products. Motorola may, at its discretion, cease providing or otherwise modify Products (or any terms related thereto in an Addendum or Proposal), in order to comply with any changes in applicable law.
- 15.2. Audit; Monitoring.** Motorola will have the right to monitor and audit use of the Products, including an audit of total user licenses credentialed by Customer for any Licensed Software or SaaS Products, which may also include access by Motorola to Customer Data and Service Use Data. Customer will provide notice of such monitoring to its Authorized Users and obtain any required consents, including individual end users, and will cooperate with Motorola in any monitoring or audit. Customer will maintain during the Term, and for two (2) years thereafter, accurate records relating to any licenses granted under this Agreement to verify compliance with this Agreement. Motorola or a third party ("Auditor") may inspect Customer's and, as applicable, Authorized Users' premises, books, and records. Motorola will pay expenses and costs of the Auditor, unless Customer is found to be in violation of the terms of the Agreement, in which case Customer will be responsible for such expenses and costs. In the event Motorola determines that Customer's usage of the Licensed Software or SaaS Product exceeded the number of licenses purchased by Customer at a given time, Motorola may invoice Customer for the additional licenses used by Customer, pro-rated for each additional license from the date such license was activated, and Customer will pay such invoice in accordance with the payment terms in the Agreement.
- 15.3. Assignment and Subcontracting.** Neither Party may assign or otherwise transfer this Agreement without the prior written approval of the other Party. Motorola may assign or otherwise transfer this Agreement or any of its rights or obligations under this Agreement without consent (a) for financing purposes, (b) in connection with a merger, acquisition or sale of all or substantially all of its assets, (c) as part of a corporate reorganization, or (d) to a subsidiary corporation. Subject to the foregoing, this Agreement will be

binding upon the Parties and their respective successors and assigns. Motorola may subcontract any of the work, but subcontracting will not relieve Motorola of its duties under this Agreement.

- 15.4. Waiver.** A delay or omission by either Party to exercise any right under this Agreement will not be construed to be a waiver of such right. A waiver by either Party of any of the obligations to be performed by the other, or any breach thereof, will not be construed to be a waiver of any succeeding breach or of any other obligation. All waivers must be in writing and signed by the Party waiving its rights.
- 15.5. Severability.** If any provision of the Agreement is found by a court of competent jurisdiction to be invalid, illegal, or otherwise unenforceable, such provision will be deemed to be modified to reflect as nearly as possible the original intentions of the Parties in accordance with applicable law. The remaining provisions of this Agreement will not be affected, and each such provision will be valid and enforceable to the full extent permitted by applicable law.
- 15.6. Independent Contractors.** Each Party will perform its duties under this Agreement as an independent contractor. The Parties and their personnel will not be considered to be employees or agents of the other Party. Nothing in this Agreement will be interpreted as granting either Party the right or authority to make commitments of any kind for the other. This Agreement will not constitute, create, or be interpreted as a joint venture, partnership, or formal business organization of any kind.
- 15.7. Third-Party Beneficiaries.** The Agreement is entered into solely between, and may be enforced only by, the Parties. Each Party intends that the Agreement will not benefit, or create any right or cause of action in or on behalf of, any entity other than the Parties. Notwithstanding the foregoing, a licensor or supplier of third-party software included in the software Products will be a direct and intended third-party beneficiary of this Agreement.
- 15.8. Interpretation.** The section headings in this Agreement are included only for convenience. The words "including" and "include" will be deemed to be followed by the phrase "without limitation". This Agreement will be fairly interpreted in accordance with its terms and conditions and not for or against either Party.
- 15.9. Notices.** Notices required under this Agreement to be given by one Party to the other must be in writing and either personally delivered or sent to the address provided by the other Party by certified mail, return receipt requested and postage prepaid (or by a recognized courier service, such as FedEx, UPS, or DHL), and will be effective upon receipt.
- 15.10. Cumulative Remedies.** Except as specifically stated in this Agreement, all remedies provided for in this Agreement will be cumulative and in addition to, and not in lieu of, any other remedies available to either Party at law, in equity, by contract, or otherwise. Except as specifically stated in this Agreement, the election by a Party of any remedy provided for in this Agreement or otherwise available to such Party will not preclude such Party from pursuing any other remedies available to such Party at law, in equity, by contract, or otherwise.
- 15.11. Survival.** The following provisions will survive the expiration or termination of this Agreement for any reason: Section 3.5 – Customer Obligations; Section 4.6 – Effect of Termination or Expiration; Section 5 – Payment and Invoicing; Section 7.9 – Warranty Disclaimer; Section 7.10 - Additional Warranty Exclusions; Section 8.3 – Customer Indemnity; Section 9 – Limitation of Liability; Section 10 – Confidentiality; Section 11 – Proprietary Rights; Data; Feedback; Section 13 – Force Majeure; Delays Caused by Customer; Section 14 – Disputes; and Section 15 – General.
- 15.12. Entire Agreement.** This Agreement, including all Addenda, and Proposals, constitutes the entire agreement of the Parties regarding the subject matter hereto, and supersedes all previous agreements, proposals, and understandings, whether written or oral, relating to this subject matter. This Agreement may be executed in multiple counterparts, and will have the same legal force and effect as if the Parties had executed it as a single document. The Parties may sign in writing or by electronic signature. An electronic signature, facsimile copy, or computer image of a signature, will be treated, and will have the same effect as an original signature, and will have the same effect, as an original signed copy of this document. This Agreement may be amended or modified only by a written instrument signed by authorized representatives

of both Parties. The preprinted terms and conditions found on any Customer purchase order, acknowledgment, or other form will not be considered an amendment or modification or part of this Agreement, even if a representative of each Party signs such document.

The Parties hereby enter into this MCA as of the Effective Date.

Motorola Solutions, Inc.

Customer: _____

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Regulated Services Addendum

This Regulated Services Addendum (this “**RSA**” or “**Addendum**”) is entered into between Motorola Solutions Connectivity, Inc. (“**MSCI**”), a wholly owned subsidiary of Motorola Solutions, Inc. (“**Motorola**”) with offices at 500 W. Monroe Street, Suite 4400, Chicago, IL 60661 and the entity set forth in the signature block below or in the MCA or Primary Agreement (“**Customer**”), and will be subject to, and governed by, the terms of the MCA or other Primary Agreement entered into between the Parties (the “**Agreement**”). Capitalized terms used in this RSA, but not defined herein, will have the meanings set forth in the Agreement or the applicable Addenda. If Customer has entered into a Subscription Software Agreement with MSCI’s parent entity, Motorola, the Parties executing this RSA agree that the terms and conditions of the Subscription Software Agreement with Motorola are adopted by MSCI and Customer and will apply to the services provided under this RSA.

1. **Scope.** This Regulated Service Addendum covers certain Services more specifically described below (the “**MSCI Services**”) and will control with respect to conflicting terms in the Agreement or any other applicable Addendum, but only as applicable to the products and Services purchased under this Addendum.
2. **MSCI Services and Compliance with Applicable Law.** MSCI shall comply with all applicable federal, state and local laws and regulations in providing the Services more fully described in Section 4 - Services and Applicable Terms and Conditions. MSCI agrees to obtain and maintain all interconnection and commercial agreements, permits, licenses, and governmental approvals necessary to perform its obligations under this Addendum. The Parties understand and agree that MSCI is Customer’s designated 9-1-1 provider for the MSCI Services contemplated under this addendum. Due the unique nature of the Services provided by MSCI, while Customer may have more than one designated 9-1-1 provider, MSCI’s foregoing designation is solely for the Services provided to Customer.
3. **Termination Charges.** If Customer terminates this MCA pursuant to Sections 4.2 or 4.3 therein, Customer shall have no further liability under this MCA except as otherwise provided in Section 4. If: (a) Customer chooses early termination of this MCA, or (b) Motorola terminates this MCA for Cause (as provided in Section 4.2), then Customer shall pay to Motorola, within thirty (30) calendar days after such termination, (i) if the termination is prior to installation of an ordered Service, an amount equal to 10% of the remaining monthly recurring charges as set forth in the pricing schedule in the applicable Proposal, or (ii) if the termination is after installation of an ordered Service, an amount equal to 50% of the monthly recurring charges as set forth in the pricing schedule in the applicable Proposal for the period remaining in the applicable Term. Notwithstanding anything to the contrary in this MCA, any non-recurring charges set forth in a pricing schedule are non-refundable.
4. **Customer Proprietary Network Information (“CPNI”).** MSCI is required by law to treat CPNI confidentially. Customer agrees that MSCI may use CPNI within its business operations, and with businesses acting on MSCI’s behalf for provision of the Services. MSCI shall protect the confidentiality of Customer CPNI in accordance with applicable laws, rules and regulations. MSCI may access, use, and disclose Customer CPNI as permitted or

required by applicable laws, rules, regulations and this Addendum.

5. **Services and Applicable Terms and Conditions.**

5.1. Vesta NXT Cloud. VESTA NXT Cloud call handling (“VESTA NXT”) is offered to Customer consistent with any Proposal documents described in the Agreement.

5.2. VESTA NXT requires network transport to transmit 9-1-1 calls from the VESTA NXT platform to the designated Customer locations. Customer agrees that it is responsible for procuring this network transport, and will provide necessary cooperation and information to MSCI in order to integrate network transport with VESTA NXT, and Customer (and/or its provider of network transport) is responsible for any and all obligations attendant to such use under applicable law. Should Customer request such network transport be provided by MSCI, it will be offered under the terms and conditions of the ESInet Services offering under this Addendum. MSCI is responsible for any regulatory obligations that are attendant to its offering, but solely for what it offers.

5.3. NGCS. Customer understands and agrees that it is responsible for ensuring that its Next Generation Core Services (“NGCS”) routing provider delivers all traffic bound for the VESTA NXT system to a mutually agreed upon point of interface that provides access to the VESTA NXT Cloud service, as defined by MSCI.

5.4. Equipment. Should Customer require equipment from MSCI and/or request to use its own equipment that will be located on Customer’s premises, MSCI may require additional terms and conditions, which will be evaluated at the time of the request and any requirements for such equipment installation will be defined in an applicable Proposal.

5.5. Emergency Backup Service (“EBS”). EBS is offered to Customer consistent with any Proposal documents described in the Agreement. Customer understands and agrees that EBS is solely offered as an emergency offering when Customer’s primary emergency call handling is unavailable. Customer use of EBS is as specifically restricted in any Proposal documents. EBS is only available if MSCI also provides the NGCS emergency call routing to Customer as more fully described in any Proposal documents.

4.5.1 EBS requires network transport to transmit 9-1-1 calls from the EBS platform to the designated Customer locations. Customer agrees that the transport used will be through public internet services, and will provide necessary cooperation and information to MSCI in order to implement EBS with necessary personnel, and Customer is responsible for any and all obligations attendant to such use under applicable law.

4.5.2. Customer agrees that EBS may not be used in any way as a standard call handling service. Should EBS be used for periods longer than those prescribed in applicable Proposal documents or otherwise in manners inconsistent with any Proposal documents, MSCI may, at its sole discretion, i) charge additional fees for use of EBS, consistent with its standard call handling offerings; ii) cease providing EBS to Customer; or iii) exercise other remedies available to MSCI, whether in law or in equity.

- 5.6. Emergency Services Internet Protocol Network ("ESInet.") ESInet is offered to Customer consistent with any Proposal documents described in the Agreement. ESInet may be obtained in conjunction with Customer's ordering of VESTA NXT and/or CCRouter from MSCI or as a standalone service, as defined in the applicable Proposal.

4.6.1. ESInet provides the physical and logical connection and data, IP, and network management services that is designed for connectivity between the MSCI VESTA NXT and/or CCRouter platforms and Customer's designated locations. Customer is responsible for providing additional wiring on its premises utilized beyond the MSCI ESInet service demarcation point. Additional wiring could entail electrical or optical cabling into 1) existing or new conduit or 2) bare placement in drop down ceilings, raised floors, or mounted to walls/ceilings. Once Service is accepted by Customer, the additional wiring then becomes property of and maintained by Customer.

4.6.2. MSCI uses different technologies to provide ESInet. Some technologies or speeds may not be available in all areas or with certain types of ESInet. MSCI utilizes different technologies to provide ESInet at its sole discretion and may include, but not be limited to ethernet, wavelength, special access, wireless technologies (again, including but not limited to LTE or equivalent wireless services or wireless satellite services). In addition, ESInet may include additional technologies for security or commonality of protocol, including but not limited to Multiprotocol Label Switching ("MPLS") and Software Defined Wide Area Network ("SD-WAN").

4.6.3. Private Port for ESInet. Private Port for ESInet includes the functionality of a Private Port and may include monitoring and notification for a MSCI provided or approved router, end-to-end performance reporting. Customer may provide a router approved by MSCI. Customer is responsible for any troubleshooting and repair of equipment on Customer's side of the MSCI ESInet service demarcation point.

4.6.4. Provisioning, Maintenance and Repair. MSCI may re-provision any local access circuits, ports or other components of ESInet from one third party provider to another and such changes will be treated as scheduled maintenance. Scheduled maintenance will not normally result in ESInet interruption. If scheduled maintenance requires ESInet interruption MSCI will: (1) provide Customer seven days' prior written notice, unless emergency or exigent circumstances apply, (2) work with Customer to minimize interruptions and (3) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time. Customer may request a technician dispatch for ESInet problems, for which MSCI will use commercially reasonable efforts to obtain applicable service from third party providers, if applicable. MSCI may assess a dispatch fee if costs for such services are invoiced to MSCI.

5. Taxes and Regulatory Cost Recovery Fees. The charges for MSCI Services do not include the following: (a) charges imposed by a third party other than MSCI (if any); (b) Taxes or Regulatory Cost Recovery Fees (as defined below); and (c) charges related to customer premises equipment or extended wiring to or at Customer premises. MSCI shall give Customer notice of such changes in rates, charges, or fees pursuant to the notice provision set forth herein or by other reasonable means. MSCI may add or adjust

rates, charges, and fees in order to recover Taxes or Regulatory Cost Recovery Fees, as defined below. Unless otherwise specified, prices do not include any excise, sales, lease, use, property, or other taxes, assessments, duties or governmental impositions including regulatory charges or contribution requirements when MSCI is required to collect such regulatory charges or contributions from Customer (collectively, "Taxes"), or any fees or charges to offset costs MSCI incurs to comply with regulations or participate in regulatory programs, including but not limited to regulatory fees or charges imposed on MSCI by governmental entities or collected from MSCI by third parties, which are not Taxes or charges that government mandates be recovered from Customer but that MSCI is permitted to recover from Customer either in aggregate or as individual line items ("Regulatory Cost Recovery Fees"). Such Taxes and Regulatory Cost Recovery Fees will be paid by Customer, except as exempt by law, unless otherwise specified in writing. If MSCI is required to pay any Taxes or permitted to recover any Regulatory Cost Recovery Fees, Customer will be billed by MSCI for such Taxes (including any interest and penalties) or Regulatory Cost Recovery Fees, whether as part of its standard billings or as separately billed and, with respect to the latter, using a "regulatory cost recovery" descriptor or other applicable descriptor, and Customer agrees that it will pay such Taxes and Regulatory Cost Recovery Fees within thirty (30) days after Customer's receipt of an invoice resulting therefrom unless Customer furnishes Motorola Solutions, Inc. or MSCI applicable tax-exemption certificates. Motorola Solutions, Inc. will be solely responsible for reporting Taxes on its income and net worth.

The Parties hereby enter into this RSA as of the date shown below.

Motorola Solutions Connectivity , Inc. **Customer:** _____

By: _____ By: _____

Name: _____ Name: _____

Title: _____ Title: _____

Date: _____ Date: _____

Section 9

Technical Matrix

Per the provided instructions, Motorola complies and has completed the Technical Matrix. Please see attachment 202691101Technical Matrix for Appendix v1 NE Motorola file 3 of 4.

Section 10

Exhibits

Exhibit 1 VESTA NXT Router NNI – Basic SIP OSP and Peer Interface Specification

VESTA NXT Router Service

Network-to-Network Interface (NNI) Specification

Basic SIP OSPs and Peer NGCS Interface

Version: 1.0

Date: July 18, 2025

TABLE OF CONTENTS

TABLE OF CONTENTS	2
EXECUTIVE SUMMARY	5
ARCHITECTURE OVERVIEW	6
Interconnection Model and Call Capacity	6
Demarcation Points	6
Connection Requirements	7
Network Protocols	7
Physical and Network Connectivity	7
Network Redundancy	7
Transport Design	8
QoS Requirements	8
Security	8
DNS and IP Addressing	9
SIP Interface	9
NEW CALL RECEIVED	9
PEER NGCS NETWORKS (Applicable to calls being transferred)	10
ASSUMPTIONS	11
Common SIP Interface Requirements	12
SIP Headers	12
Supported SIP Error Codes	15
Media Interface	16
RTP	16
MSRP	16
RTT	16
Examples	17
[Incoming] INVITE for a Basic SIP Call	17
[Incoming] INVITE for an MSRP Text-to-911	17
a=path:msrp://10.179.8.13:6002/Zf8mgnYpzLU;tcp	18
[Outgoing] INVITE for a Neighbor Basic SIP Router - PSAP Transfer	18
MSRP Message	18
MSRP Handshake Message	18
REFERENCE DOCUMENTS	19
ACRONYMS	20

APPENDIX	22
APPENDIX 1 : RFC DESCRIPTIONS	22

Document Release Notes:

Date	Version	Release Notes Description
July 18, 2025	1.0	Initial document release

EXECUTIVE SUMMARY

This document establishes interface specifications for Originating Service Providers (OSPs) and other NG9-1-1 Service Providers interconnecting to the VESTA NXT Router for calls handoff and/or calls transfer using basic SIP.

The scope of this document is to provide a specification of SIP and RTP protocols that provides equivalency to a 9-1-1 Selective Router to 9-1-1 Selective Router SS7 interface and an OSP delivering calls to a 9-1-1 Selective Router.

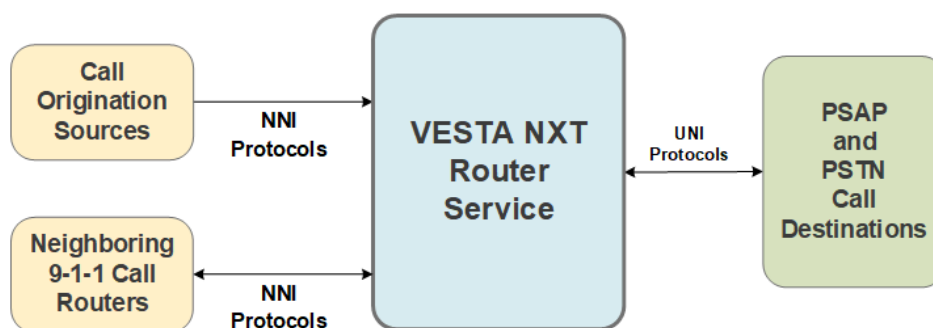
Basic SIP replaces legacy TDM facilities with the benefits of IP, eliminating point to point TDM trunks and gaining the benefits of IP transport technologies. Basic SIP does not attempt to be functionally equivalent to NENA i3 functionality or protocols. A Basic SIP OSP interface assumes the OSP is using DBMS services to provide ALI and/or pANI records to the 9-1-1 call routing operating environment.

Throughout the document, the reference to OSP is used in a generic way to encompass true Originating Service Providers as well as, depending on the context, peer networks ingressing or transferring calls to the VESTA NXT Router.

Detailed specifications for DNS support and IPv6 support are the objective guidelines. Currently it is understood that not all cases and deployments are fully compliant.

The following diagram illustrates the context of the Basic SIP NNI protocol presented in this document.

VESTA NXT Router Service Context Diagram

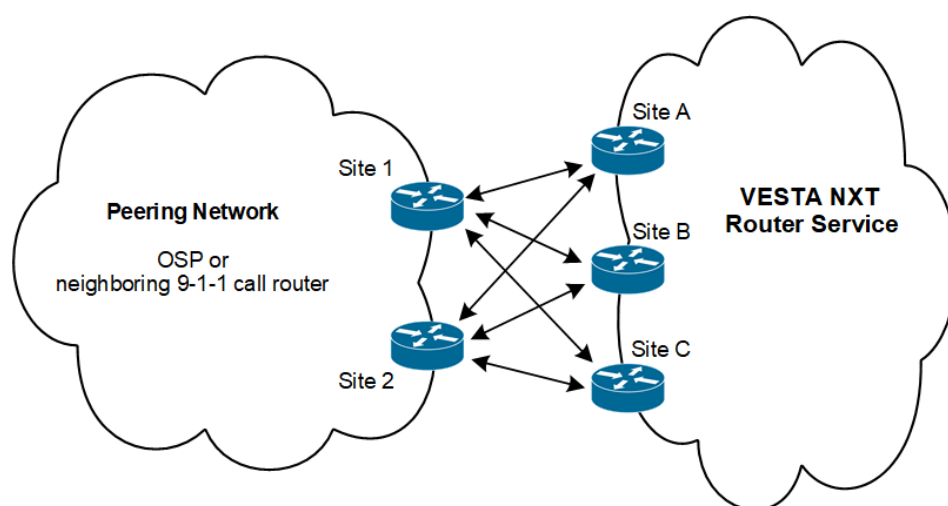


ARCHITECTURE OVERVIEW

Interconnection Model and Call Capacity

Interconnection between the Peering Network (OSP, Aggregator or other ESInet) and an instance of VESTA NXT Router should be a redundant interconnection model as illustrated (as an example) in the following diagram.

**Fully Redundant Interconnection Model
VESTA NXT 3 interconnection points**



Capacity, or number of simultaneous calls, between the Peering Network and the VESTA NXT Router instance is determined by mutual agreement. There is currently no programmatic method to enforce a call volume limit (other than the receiving entity responding with a SIP messaging to reject calls above some threshold) and it is expected each entity will cooperatively use the facilities per agreements. Denial of Service (DOS) attacks or similar network scenarios will be handled according to the entity's network management functions.

Demarcation Points

For the scope of this document, the pertinent demarcation points are the borders between the VESTA NXT Router domain and the OSP, Selective Router and Peer NGCS domains as represented in the diagram above.

Connection Requirements

Network Protocols

SIP interconnection allows OSP's to deliver 9-1-1 calls via IP to the VESTA NXT Router network, which will then result in the call being routed to the appropriate answering point. VESTA NXT Router presently supports only IPv4.

VESTA NXT Router implementation of SIP is based on RFC-3261 (SIP: Session Initiation Protocol) and RTP implementation is based on RFC-3550 (RTP: A Transport Protocol for Real-Time Applications). The VESTA NXT Router also supports many other RFCs listed in the annexe section.

If the need arises to support services and protocols such as 183 - early media or provisional ACKs, these specifics can be negotiated.

Physical and Network Connectivity

VESTA NXT Router requires each SIP OSP (or OSP aggregator) to deliver their 9-1-1 originated calls via dedicated IP circuits to each of the specified VESTA NXT Router Points of Interconnect (POI) for the service area.

VESTA NXT Router preference is for a copper Ethernet handoff via a standard RJ-45 connector. VESTA NXT Router can also support Ethernet over single mode fiber optic media with LC connectors. The OSP is responsible for establishing a cross connect to the VESTA NXT Router demarc.

SIP is expected to use the standard port of 5060 (5061 for SIP over TLS). RTP will use a UDP port range determined by the OSP and agreed upon by VESTA NXT Router. OSPs connecting to VESTA NXT Router via SIP should expect to see these ports advertised from VESTA NXT Router SBCs.

The OSPs will implement a SIP failover design to each of VESTA NXT Router geographically diverse data centers. This ensures any 9-1-1 call can be delivered to VESTA NXT Router, even in the event of a disruption to one OSP connection to a VESTA NXT Router data center.

Network Redundancy

The VESTA NXT Router ESInet is a completely redundant, geo-diverse environment. It is expected that Originating Service Providers (OSPs) and other NG9-1-1 Service Providers are connecting to the VESTA

NXT Router NG9-1-1 network at a minimum of two of its POI locations and that each connection is capable of supporting the entire volume of 9-1-1 calls.

Transport Design

1. The transport protocol for SIP shall be TCP using predefined source IPv4 addresses. Use of TLS is optional.
2. VESTA NXT Router requires IP interconnection to be implemented with IPv4 and VPNs. Use of IPv6 must be negotiated on a deployment basis. SIPs (RFC 3261) and SRTP (RFC 3711) as a substitution for a VPN connection is on a mutual agreement basis.
3. RTP media packets are transported with UDP
4. Network infrastructure supports MTU of 1500 bytes which has been defined as the standard MTU by the NENA specifications for Next-Generation 9-1-1 services.
5. If TLS is used, Peering Network calls to VESTA NXT Router may use either one TLS connection for all the dialogs or a separate TLS connection per each dialog (preferred solution).
6. If TLS is used, The VESTA NXT Router shall reuse the TLS connection(s) for all SIP responses and new SIP requests in the same dialog.
7. If TLS is used, in case of a connection failure:
 - a. VESTA NXT Router shall establish a new TLS connection towards the originating Peering Network using the connection parameters advertised by the ingressing calls in SIP headers (Via or Contact).

QoS Requirements

The VESTA NXT Router is implementing QoS policies (including traffic DSCP marking) to meet packet delivery criteria as measured in terms of Jitter, Latency and Packet Loss. VESTA NXT Router will mark packets and perform traffic conditioning according to NENA i3 specifications [\[NENA-STA-010.3\]](#). The Peering Network is responsible for their own QoS performance up to the VESTA NXT Router POI.

Security

VESTA NXT Router incorporates SBCs and Firewalls per NENA-STA-010.3.

Certificate establishment and key exchange algorithms must support PFS (Perfect Forward Secrecy). Upon establishing interconnection agreements VESTA NXT Router and Peering Network will establish security certificates issuing, deployment and agree upon renewal processes.

See the section above "[Transport Design](#)" for a discussion regarding VPN connection and SIPs and SRTP protocols.

All HTTP connections utilize HTTPS (HTTP/TLS (RFC 2818)).

DNS and IP Addressing

Both VESTA NXT Router and Peering Network are required to resolve URIs sent via SIP protocol and URLs sent via HTTPS protocol using DNS. VESTA NXT Router utilizes public IP addresses that are only routable over private dedicated connections and are not reachable from the Internet. VESTA NXT Router supports DNS SRV records and does not provide NAPTR records.

The Peering Network is required to provide its own DNS.

SIP Interface

NEW CALL RECEIVED

Emergency calls originating from service providers unable to comply with ATIS-0700015 (which are referred to as "Basic SIP") must format their emergency calls as follow:

- Request URI must contain the target VESTA NXT Router ESRP queue URI containing a DRI in the user part of the URI.
- INVITE should include a P-Asserted-Identity header (E.164 SIP URI format) containing a number which will be used as a location lookup key (such as in an ALI database). If the PAI header is not provided, then this number must be included in the From header.

Note: The Request URI fields can be used to proceed to default routing if required. Any originating service (e.g., OSP or traffic aggregation service) that obscures a legacy ingress trunk group (e.g., consolidates traffic into a SIP trunk that would otherwise be recognizable to the ESRP as a physical trunk group and assigned a default route) must include a DRI. The DRI value is assigned by MSI.

PEER NGCS NETWORKS (Applicable to calls being transferred)

If the peer 9-1-1 network's signaling is pre-i3, then the calls originating from that network (which are referred to as Basic SIP or just SIP) must be as follow:

- Request URI must contain the target VESTA NXT Router ESRP queue URI
- INVITE should include a P-Asserted-Identity header (E.164 SIP URI format) containing a number which will be used as a location lookup key (such as in an ALI database). If the PAI header is not provided, then this number must be included in the From header.

ASSUMPTIONS

1. SIP Back-to-Back User Agent (B2BUA) functions can be used in support of network interconnection.
2. It is expected that DTMF tones are transported as RTP Events (following RFC-4733 which replaces RFC-2833). DTMF will be transported using RTP Events if generated by the originating entity. DTMF tones embedded within the RTP audio stream will not be detected and converted to RTP Events by VESTA NXT Router.
3. Elements ingressing calls shall allow configuration of the SIP Timer_B (Call Setup Time). Due to the emergency nature of provided call service, default SIP call timers are not satisfactory (i.e. users cannot wait 30 seconds for a ringtone.).
4. Elements ingressing calls shall support "SIP 302 Moved Temporarily" message according to RFC 3261.
5. Elements ingressing calls shall maintain the connection via heartbeat mechanism using SIP OPTIONS by both sending and responding to these SIP OPTIONS (during periods of inactivity).
6. Elements ingressing calls shall use SIP re-INVITE messages for SIP session keep-alive according to RFC 4028.
7. Elements ingressing calls will be provided with VESTA NXT Router FQDN which must be resolved using DNS SRV records when sending SIP requests/responses. Elements ingressing calls shall try each address found in SRV records until a VESTA NXT Router is contacted (according to RFC 3261 and RFC 3263).
8. In order to support Basic SIP between two 911SSPs, the sharing of ALI LDB records or requiring OSPs to dual provision is required. This sharing, when achieved from a configuration point of view shall be standardized using the NENA 2.1 format.

Common SIP Interface Requirements

Basic SIP uses the called number from the user part of the Request URI to determine the call processing function, either route (including default route) or transfer.

The VESTA NXT Router attempts to map the called number field to a RDN or a DRI (a DRI conveys the relationship between an OSP's ingress trunk group and a Default Routing policy). If it maps to a RDN, the VESTA NXT Router will send the call to the corresponding PSAP. If it maps to a DRI, the call will follow geo routing and if the routing attempt fails the call is then Default Routed where the DRI value indicates the target PSAP.

See the examples section for different Request URI depending on call type.

SIP Headers

Header	Basic SIP	Reference	Details
Accept	Optional	RFC 3261 Section 20.1	Example: Allow: INVITE, ACK, OPTIONS, PRAC, BYE
Allow	Optional	RFC 3261 Section 20.5	Shall be present in the initial INVITE and its associated 200-OK response. Example: Allow: INVITE, ACK, OPTIONS, PRAC, BYE
Call-ID	Mandatory	RFC 3261 Section 20.8	Example: Call-ID: cb03a0b53
Contact	Mandatory	RFC 3261 Section 20.10	If the originator of the call is capable of processing conference-related REFER requests then "isfocus" parameter must be specified. The Parties will mutually agree upon implementation of this i3 SIP function.
ContentLength	Conditional	RFC 3261 Section 20.14	Must be present if there is a SIP body. Example: 256
Content-Type	Conditional	RFC 3261 Section 20.15	Must be present if there is a SIP body with a MIME type.

			Example: Content-Type: multipart/mixed; boundary=boundary1
CSEQ	Mandatory	RFC 3261 Section 20.16	
From	Mandatory	RFC 3261 Section 20.20	Must contain ANI (wireline), pANI (wireless) or Callback (i2/VoIP). Examples: From:<sip:3125551234@carrier.example.co m;user=phone>;tag=171828 From:<tel:3125551234>;tag=171828
History-Info	Passthrough	RFC 4244	History-Info headers are passed through if received from a Neighbor i3 Router.
Max-Forwards	Mandatory	RFC 3261 Section 20.22	Example: Max-Forwards: 70
MIME-Version	Optional	RFC 3261 Section 20.24	Present if there is a SIP body with a MIME type. If none, version 1 will be assumed. Example: MIME-Version: 1.0
P-Access-Network-Info	Passthrough	RFC 3455	May indicate cell site. Example: P-Access-Network-Info:3GPP-E-UTRAN-FDD ;utran-cell-id-3gpp=0AE212345608A41F9
P-Asserted-Identity	Conditional	RFC 3325	In the case signaling includes both a pANI and a callback number, the P-Asserted-Identity field must be the callback number of the call unless i2 signaling where it must be the pANI.

			Example: P-Asserted-Identity:<sip:+13125551234@carrier.example.net;user=phone>
P-ChargingVector	Passthrough	RFC 3455	May identify the originating carrier. Example: P-Charging-Vector:icid=34c23c445902;idid-generatedat=ecscf.carrier.example.net;orig-ioi=carrier.example.net
P-PreferredIdentity	Passthrough	RFC 3325	Example: P-Preferred-Identity:<sip:+13125551234@carrier.example.net;user=phone>
Record-Route	Optional	RFC 3261 Section 20.30	Example: Record-Route:<sip:sbc.carrier.example.com;lr>
Supported	Optional	RFC 3261 Section 20.37	Example: Supported: geolocation
To	Mandatory	RFC 3261 Section 20.39	Specifies a recipient of a SIP request
Unsupported	Optional	RFC 3261 Section 20.40	Example: Unsupported: geolocation
Via	Mandatory	RFC 3261 Section 20.42	Example: Via:SIP/2.0/UDP[aaa:bbb:ccc:ddd]:1357;branch=z9hG4bKnashds7

Supported SIP Error Codes

SIP Error Code	Description
400	Bad Request
404	Not Found
405	Method Not Allowed
406	Not Acceptable
422	Session Interval Too Small
423	Interval Too Brief
481	Call/Transaction Does Not Exist
482	Loop Detected
483	Too Many Hops
484	Address Incomplete
486	Busy Here
487	Request Terminated
488	Not Acceptable Here
489	Bad Event
491	Request Pending
500	Internal Server Error
501	Not Implemented
504	Server Time-out
600	Busy Everywhere
604	Does Not Exist Anywhere

Media Interface

If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

RTP

VESTA NXT Router only supports G.711 uLaw codec with a 20ms packetization rate. It is expected that interconnecting networks not use silence suppression.

Media interface shall use RTP protocol (RFC 3550) over UDP. Note:

VESTA NXT Router implements a call disconnect (session termination) function upon Loss of RTP (> 30 seconds).

MSRP

The media type for Text-to-911 calls is MSRP. MSRP utilizes TCP as the transport protocol. All previous SIP messages and interaction description apply specific to VESTA NXT Router receiving 9-1-1 calls or Neighbor i3 Router interactions.

RTT

The media type and interaction models for Real Time Text (RTT) 9-1-1 calls. RTT will be documented in a future NNI specification version.

Examples

The messages in this section are provided as examples and the implementations may not contain all fields described here.

[Incoming] INVITE for a Basic SIP Call

```

INVITE sip:1230590992@esrp.msi-ngcs.com:5060 SIP/2.0
Via: SIP/2.0/TCP 206.147.246.140:5060;branch=z9hG4bK0cB504ae8f871de4369
From: <sip:+11661460017@206.147.246.140;isup-oli=00>;tag=gK0c3e077f
To: <sip:1230590992@131.197.49.105>
Call-ID: 390858894_113234721@206.147.246.140
CSeq: 1 INVITE
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,PRACK,UPDATE,OPTIONS,MESSAGE,PUBLISH
Accept: application/sdp
Contact: <sip:911@206.147.246.140:5060;transport=tcp>
P-Asserted-Identity: <sip:+11661460017@206.147.246.140:5060>
Supported: timer,100rel
Session-Expires: 1800
Min-SE: 90
Content-Length: 241
Content-Type: application/sdp

v=0
o=Sonus_UAC 610393 468415 IN IP4 206.147.246.140
s=SIP Media Capabilities
c=IN IP4 206.147.246.134
t=0 0
m=audio 23338 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
a=ptime:20

```

[Incoming] INVITE for an MSRP Text-to-911

```

INVITE sip:1230590992@esrp.msi-ngcs.com:5060 SIP/2.0
Via: SIP/2.0/TCP 206.147.246.140:5060;branch=z9hG4bK0cB504ae8f871de4369
From: <sip:+1661460017@206.147.246.140;isup-oli=00>;tag=gK0c3e077f
To: <sip:1230590992@131.197.49.105>
Call-ID: 390858894_113234721@206.147.246.140
CSeq: 1 INVITE
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,PRACK,UPDATE,OPTIONS,MESSAGE,PUBLISH
Accept: application/sdp
Contact: <sip:911@206.147.246.140:5060;transport=tcp>
P-Asserted-Identity: <sip:+1661460017@206.147.246.140:5060>
Supported: timer,100rel
Session-Expires: 1800
Min-SE: 90
Content-Length: 241
Content-Type: application/sdp

v=0
o=- 1728493043519 1 IN IP4 0.0.0.0
s=-
c=IN IP4 10.179.8.13
t=0 0
m=message 6002 TCP/MSRP *
a=accept-types:text/plain

```


a=setup:active
a=path:msrp://10.179.8.13:6002/Zf8mgnYpzLU;tcp

[Outgoing] INVITE for a Neighbor Basic SIP Router - PSAP Transfer

INVITE sip:1230590002@neighbour.router.com SIP/2.0
Via: SIP/2.0/TCP 131.197.42.41:5060;alias;rport;branch=z9hG4bKac1032354063
Max-Forwards: 69
From: <sip:1420599901@esrp.msi-ngcs.com>;tag=1c901993876
To: <sip:1230590002@neighbour.router.com>
Call-ID: 85e9899c-5db4-4315-adc6-a7f70d2dd610@esrp.msi-ngcs.com
CSeq: 1 INVITE
Contact: <sip:6b41f461-c4b7-4cb8-8995-0c07a4772378@131.197.42.41:5060;transport=tcp>
Supported: timer,sdp-anat
Allow: INVITE,ACK,CANCEL,BYE,REFER,OPTIONS,NOTIFY,SUBSCRIBE,UPDATE
Session-Expires: 3600;refresher=uas
Min-SE: 90
Referred-By: <sip:psap.fire@msi-ngcs.com>
User-Agent: Mediant CE SBC/v.7.40A.600.231
P-Asserted-Identity: <sip:+18722687001@esrp.msi-ngcs.com>
Call-Info: <urn:emergency:uid:incidentid:1752845360613sosbt5pap1lw:esrp.msi-ngcs.com>;purpose=emergency-IncidentId
Call-Info: <urn:emergency:uid:callid:17528453606131lnagkna556z:esrp.msi-ngcs.com>;purpose=emergency-CallId

Content-Type: application/sdp
Content-Length: 265
v=0
o=CCMediaServer 1730243950 919874208 IN IP4 131.197.42.39
s=CCMediaServer
c=IN IP4 131.197.42.39
t=0 0
m=audio 23984 RTP/AVP 0 101
c=IN IP4 131.197.42.39
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtcp:23985
a=fmtp:101 0-15

MSRP Message

MSRP WIwI0im1TiPM SEND
To-Path: msrp://10.65.54.159:27000/k0h2E000;tcp
From-Path: msrp://131.197.49.105:5500/gJW86fptYz4dp;tcp
Message-ID: vUpVU0wcuKzt
Byte-Range: 1-15/15
Content-Type: text/plain text/x-msrp-heartbeat

Are you there?

-----WIwI0im1TiPM\$

MSRP Handshake Message

MSRP MgTqxKDJHeBjHT9i SEND
To-Path: msrp://10.65.54.159:27000/k0h2E000;tcp
From-Path: msrp://131.197.49.105:5500/gJW86fptYz4dp;tcp
Message-ID: AuL8T2TJRNdLlBj
Byte-Range: 1-0/0
Content-Type: text/plain
-----MgTqxKDJHeBjHT9i\$

REFERENCE DOCUMENTS

- [NENA-STA-010.2](#) Detailed Functional and Interface Specification for the NENA i3 Solution
- ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination (document number [ATIS-0700015](#))
- [NENA-INF-016.2-2018](#) Emergency Services IP Network Design (ESIND) Information Document
- International Telecommunications Union (ITU) One-way Transmission Time ([G.114](#))

ACRONYMS

Acronym	Definition
ADR	Additional Data Repository
ATIS	Alliance for Telecommunications Industry Solutions
BCF	Border Control Function
CLEC	Competitive Local Exchange Carrier
CO	Central Office
DNS	Domain Name Service
DRI	Default Route Identifier
DSCP	Differentiated Services Code Point
ECRF	Emergency Core Routing Function
ESInet	Emergency Services Internetwork
ESRP	Emergency Services Routing Proxy
HELD	HTTP-Enabled Location Delivery
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standards
IT	Information Technology
ITU	International Telecommunication Union
LDB	Legacy Database
LIS	Location Information Service
LRF	Location Retrieval Function
MPLS	Multiprotocol Label Switching
MTU	Message Transfer Unit
NENA	National Emergency Number Association
NGCS	Next Generation Core Services
NIST	National Institute of Standards and Technology

NNI	Network-to-Network Interface
OSP	Originating Service Provider
POI	Point of Interconnection
PRF	Policy Routing Function
PRR	Policy Routing Rules
PSAP	Public Safety Answering Point
QoS	Quality of Service
RDF	Routing Determination Function
RDN	Routing Directory Number / ReDirection Number
RTT	Real-time Text
SBC	Session Border Controller
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier

APPENDIX

APPENDIX 1 : RFC DESCRIPTIONS

[RFC-2475](#): An Architecture for Differentiated Services

[RFC-2818](#): HTTP Over TLS

[RFC-2833](#): RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

[RFC-3261](#): SIP: Session Initiation Protocol

[RFC-3262](#): Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

[RFC-3263](#): Session Initiation Protocol (SIP): Locating SIP Servers

[RFC-3264](#): An Offer/Answer Model with the Session Description Protocol (SDP)

[RFC-3311](#): The Session Initiation Protocol (SIP) UPDATE Method

[RFC-3323](#): A Privacy Mechanism for the Session Initiation Protocol (SIP)

[RFC-3325](#): Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

[RFC-3326](#): The Reason Header Field for the Session Initiation Protocol (SIP)

[RFC-3398](#): Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping

[RFC-3455](#): Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)

[RFC-3515](#): The Session Initiation Protocol (SIP) Refer Method

[RFC-3525](#): Gateway Control Protocol Version 1

[RFC-3550](#): RTP: A Transport Protocol for Real-Time Applications

[RFC-3711](#): The Secure Real-time Transport Protocol (SRTP)

[RFC-3761](#): The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)

[RFC-3824](#): Using E.164 numbers with the Session Initiation Protocol (SIP)

[RFC-3891](#): The Session Initiation Protocol (SIP) “Replaces” Header

[RFC-3966](#): The tel URI for Telephone Numbers

[RFC-4028](#): Session Timers in the Session Initiation Protocol (SIP)

[RFC-4033](#): DNS Security Introduction and Requirements

[RFC-4034](#): Resource Records for the DNS Security Extensions

[RFC-4035](#): Protocol Modifications for the DNS Security Extensions

[RFC-4244](#): An Extension to the Session Initiation Protocol (SIP) for Request History Information

[RFC-4317](#): Session Description Protocol (SDP) Offer/Answer Examples

[RFC-4488](#): Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription

[RFC-4566](#): SDP: Session Description Protocol

[RFC-4694](#): Number Portability Parameters for the “tel” URI

[RFC-4733](#): RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

[RFC-4904](#): Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)

[RFC-5031](#): A Uniform Resource Name (URN) for Emergency and Other Well-Know Services

[RFC-5923](#): Connection Reuse in the Session Initiation Protocol (SIP)

[RFC-6442](#): Location Conveyance for the Session Initiation Protocol

[RFC-6665](#): (Future) SIP-Specific Event Notification

[RFC-6881](#): Best Current Practice for Communicating Services in Support of Emergency Calling

[RFC-7852](#): Additional Data Related to an Emergency Call

Exhibit 2 VESTA NXT Router NNI Specification – i3 SIP OSP and Neighbor i3 Router

VESTA NXT Router Service

Network-to-Network Interface (NNI) Specification

i3 SIP OSPs Neighbor i3 Router

Version: 1.1

Date: July 18, 2025

Table of Contents

Executive Summary	5
Acronyms / Definitions	6
Architecture Overview	7
Interconnection Model and Call Capacity	8
Connection Requirements	10
Physical and Network Connectivity	11
Network Protocols	11
Transport Design	11
QoS Requirements	12
Security	12
DNS and IP Addressing	12
SIP Interface	12
Common SIP Interface Requirements	13
Calls Delivered to VESTA NXT Router Service for Routing	15
Call Hand-off with Neighbor i3 Router	15
Neighbor Call Router - Call Loop Prevention	16
Neighbor i3 Router Interactions - Call Transfer	16
SIP Headers	17
Media Interface	21
RTP	21
MSRP	21
RTT	21
HELD & HTTPs Additional Data Interfaces	22
Supported SIP Error Codes	22
Examples	23
INVITE for a fixed location 9-1-1 call - LbV	23
INVITE for an ATIS-0700015 Wireless Call - LbV and LbR	25
INVITE for an MSRP Text-to-911	27
INVITE for a Neighbor i3 Router - Call Hand-off	27
INVITE for a Neighbor i3 Router - PSAP Transfer	28
HELD locationResponse Example	29
ADR Response – Provider Info Example	29
ADR Response – Service Info Example	31
ADR Response – Device Info Example	31
ADR Response – Comment Example	32
ADR Response – Subscriber Info Example	32

MSRP Message	34
MSRP Handshake Message	34
Appendices	35
Reference Documents	35
IETF RFC Standard References	35

Document Release Notes:

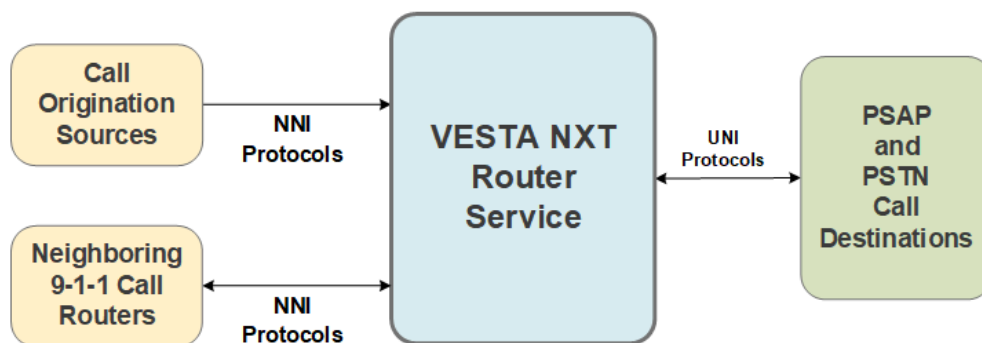
Date	Version	Release Notes Description
February 8, 2024	1.0	Initial VESTA NXT Router Service i3 NNI document release
July 18, 2025	1.1	Updated protocol messages examples

Executive Summary

This document establishes the interface specification for Originating Service Providers (OSPs) and Neighbor i3 Router service providers interconnecting to VESTA NXT Router Service. OSPs interconnect for 9-1-1 call delivery to VESTA NXT Router. OSPs deliver 9-1-1 calls to VESTA NXT Router and provide 9-1-1 call related data information via LIS and ADR web services.

Neighbor i3 Router service providers interconnect for call hand-off scenarios and/or calls transfer scenarios. VESTA NXT Router may receive calls from or deliver calls to a Neighbor i3 Router service. Calls received by either entity, VESTA NXT Router or a Neighbor i3 Router, could be received from a legacy OSP that does not implement i3 services but the initial 9-1-1 call router still presents i3 service interfaces for each call to the downstream 9-1-1 call router.

VESTA NXT Router Service Context Diagram



The VESTA NXT Router ESInet is a completely redundant and geo-diverse 9-1-1 call routing operating environment. Interconnections are required to support redundancy and call load distribution to minimize possible 9-1-1 call processing impacts.

This document is not intended to provide a detailed overview of the functionality of NG9-1-1 or to cover details already specified in existing normative references (e.g., NENA or ATIS standards). The NENA i3 standard should be viewed as the normative default standard unless otherwise specified by this document.

The National Emergency Number Association (NENA) i3 standard defines how emergency IP-based 9-1-1 calls from OSPs are routed to determine the most appropriate PSAP. 9-1-1 calls are routed based on the location that is associated with the call. Therefore, it is required that all calls presented to VESTA NXT Router be supported with caller location information. In addition, the NENA i3 standard defines

how different NGCS networks must interconnect in order to allow NG9-1-1 calls to be exchanged between the networks.

In addition to NENA i3, OSP related interface standards are defined in two references:

1. The Internet Engineering Task Force (IETF) Best Current Practice for Communications Services in Support of Emergency Calling ([RFC6881](#)).
2. The [Alliance for Telecommunications Industry Solutions](#) (ATIS) is the normative body responsible for OSPs and has developed to the ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination ([ATIS-0700015](#)).

Acronyms / Definitions

Acronym	Definition
ADR	Additional Data Repository
ATIS	Alliance for Telecommunications Industry Solutions
BCF	Border Control Function
CLEC	Competitive Local Exchange Carrier
CO	Central Office
DNS	Domain Name Service
DSCP	Differentiated Services Code Point
ECRF	Emergency Core Routing Function
EIDO	Emergency Incident Data Object
ESInet	Emergency Services Internetwork
ESRP	Emergency Services Routing Proxy
HELD	HTTP-Enabled Location Delivery
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standards
IT	Information Technology
ITU	International Telecommunication Union
LDB	Legacy Database

© 2020-2025 Motorola Solutions Connectivity, Inc. and Motorola Solutions Connectivity of Virginia, Inc., wholly owned subsidiaries of Motorola Solutions, Inc. This document is protected by copyright law and international treaties, and is the CONFIDENTIAL AND PROPRIETARY information of Motorola Solutions Connectivity, Inc. All trademarks, service marks, product names, brands, company names and logos appearing in this document are the property of their respective owners. VESTA® is a registered trademark of Motorola Solutions Connectivity, Inc.

© 2020-2025, Motorola Solutions. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

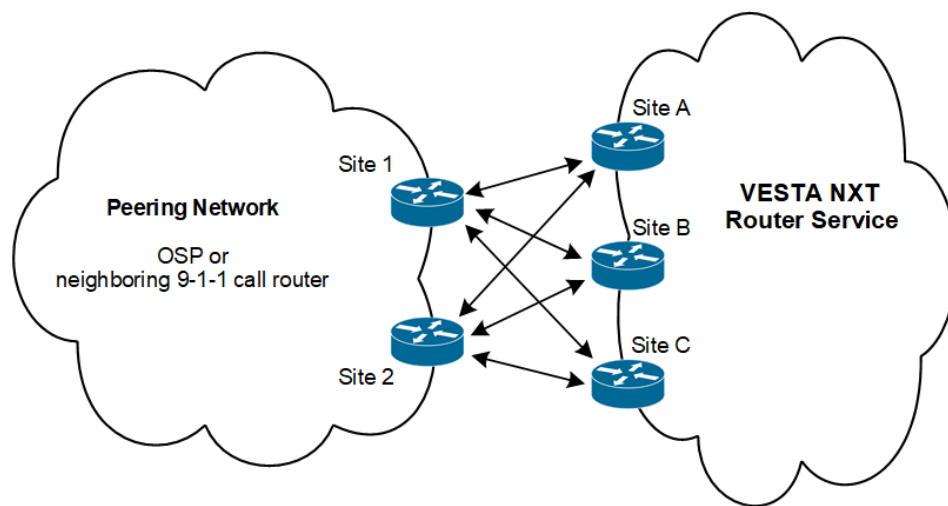
LIS	Location Information Service
LRF	Location Retrieval Function
MPLS	Multiprotocol Label Switching
MTU	Message Transfer Unit
NENA	National Emergency Number Association
NGCS	Next Generation Core Services
NIST	National Institute of Standards and Technology
NNI	Network-to-Network Interface
OSP	Originating Service Provider
Peering Network	An Entity, OSP or Neighbor i3 Router, interconnecting to VESTA NXT Router Service.
POI	Point of Interconnection
PRF	Policy Routing Function
PRR	Policy Routing Rules
PSAP	Public Safety Answering Point
QoS	Quality of Service
RDN	Routing Directory Number / ReDirection Number
RTT	Real-time Text
SBC	Session Border Controller
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier

Architecture Overview

Interconnection Model and Call Capacity

Interconnection between a Peering Network (OSP or Neighbor i3 Router) and VESTA NXT Router is a redundant interconnection model as illustrated in the following diagram. Each Peering Network is required to interconnect at two distinct and redundant Points of Interface (POIs). These POIs should be geographically distributed to mitigate the possibility of a failure causing service disruption.

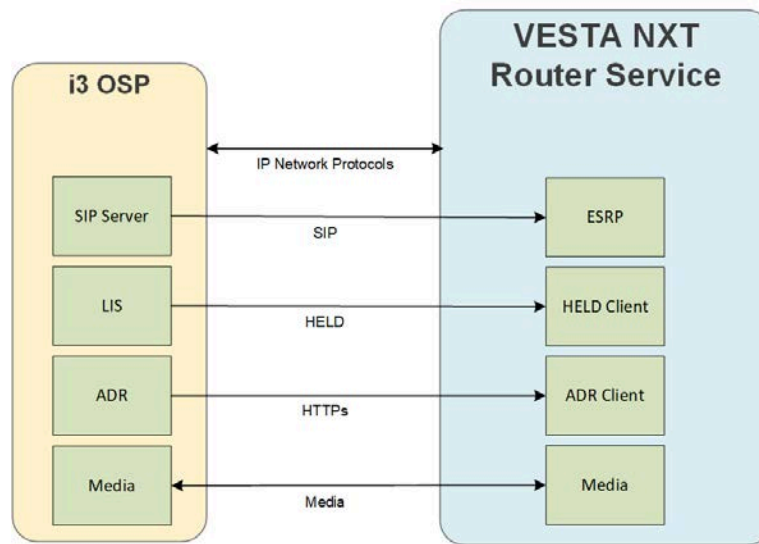
Fully Redundant Interconnection Model
VESTA NXT 3 interconnection points



Capacity, or number of simultaneous calls, between the Peering Network and VESTA NXT Router is determined by mutual agreement. Simultaneous calls (SIP INVITEs) volume is limited by the receiving entity responding with a SIP message to reject calls above some predetermined threshold. It is expected each entity will cooperatively use the facilities per agreements. Denial of Service (DOS) attacks or similar network scenarios are to be handled according to the entity's network policies.

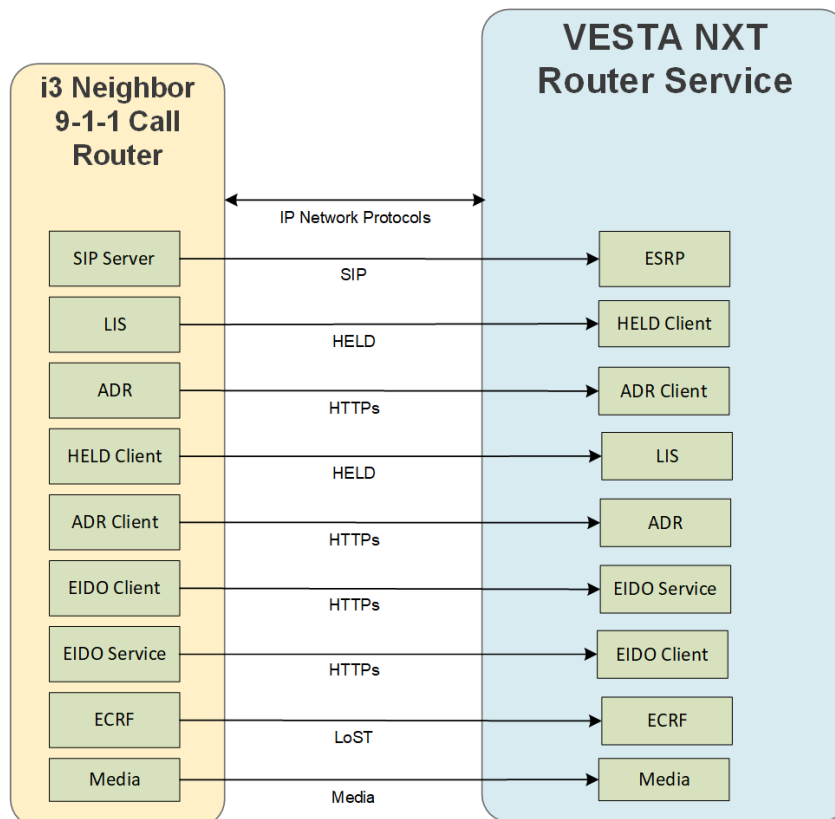
The following diagram illustrates the functional entity interactions and corresponding protocols between an i3 OSP operating environment and VESTA NXT Router. The IP Network Protocols represented by “IP Network Protocols” include Layer 3 eBGP Peering.

VESTA NXT Router Service i3 OSP NNI Protocols



The next diagram illustrates the functional entity interactions and corresponding protocols between a neighbor i3 9-1-1 call router and VESTA NXT Router. This scenario includes the ability for VESTA NXT Router to exchange (receive and deliver) calls and data with neighbor i3 9-1-1 call routers.

i3 Neighbor Call Router NNI Protocols



Connection Requirements

VESTA NXT Router requires each Peering Network to deliver their 9-1-1 originated calls to specified VESTA NXT Router Points of Interconnect (POI). The POIs are required to be geographically distributed and redundant to each other. The POIs are to be active-active and NOT operated in an active-standby fashion. Both links should carry transaction traffic over a relative period of time to verify that each link is functionally capable. Interconnecting Peering Networks are expected to implement a SIP failover design between the interconnection POIs.

VESTA NXT Router requires each Peering Network to provide predetermined URI queue names for specific situations. Queue names are conveyed in the SIP INVITE message topmost Route header as

described below. Queue names will be established by mutual agreement between the interconnecting parties. 9-1-1 calls sent to VESTA NXT Router must provide a queue name representative of the target customer service area (PSAP or 9-1-1 Jurisdiction). This queue name strategy allows VESTA NXT Router to implement a 9-1-1 call default location and default routing strategy according to NENA i3 requirements. A given Peering Network may direct calls to many different VESTA NXT Router queue URIs and should support multiple VESTA NXT Router queue URIs for different geographic 9-1-1 caller areas.

A Neighbor i3 Router may implement call hand-off and/or “PSAP to PSAP” call transfer scenarios. For a 9-1-1 call hand-off scenario the queue name will indicate to VESTA NXT Router to route the call via nominal routing algorithms. A PSAP specific URI queue name will cause VESTA NXT Router to deliver the call to the corresponding PSAP. In some scenarios, the originator may receive a SIP 4xx message.

Physical and Network Connectivity

Specific physical network interconnection will be negotiated for each specific situation. Physical interconnection typically includes either single or dual mode fiber optic media 100Base-FX or copper Ethernet RJ-45 connector hand-off. The Peering Network is responsible for establishing a cross connect to the VESTA NXT Router demarc.

Network Protocols

VESTA NXT Router implements Layer 3 eBGP Peering with Peering Network providers.

Transport Design

1. VESTA NXT Router requires IP interconnection to be implemented with IPv4 and VPNs. Use of IPv6 must be negotiated on a deployment basis. SIPs (RFC 3261) and SRTP (RFC 3711) as a substitution for a VPN connection is on a mutual agreement basis.
2. RTP media packets are transported with UDP. SRTP is not supported.
3. Network infrastructure supports MTU of 1500 bytes which has been defined as the standard MTU by the NENA specifications for Next-Generation 9-1-1 services.
4. If TLS is used, Peering Network calls to VESTA NXT Router may use either one TLS connection for all the dialogs or a separate TLS connection per each dialog (preferred solution).
5. If TLS is used, The VESTA NXT Router shall reuse the TLS connection(s) for all SIP responses and new SIP requests in the same dialog.
6. If TLS is used, in case of a connection failure:
 - a. VESTA NXT Router shall establish a new TLS connection towards the originating Peering Network using the connection parameters advertised by the ingressing calls in SIP headers (Via or Contact).

If a TLS connection fails the transaction should attempt a TCP connection.

For LbR, the HTTPS URL must be reachable over the same IP interconnect points used to facilitate SIP signaling and may be globally routable.

QoS Requirements

The VESTA NXT Router is implementing QoS policies (including traffic DSCP marking) to meet packet delivery criteria as measured in terms of Jitter, Latency and Packet Loss. VESTA NXT Router will mark packets and perform traffic conditioning according to NENA i3 specifications [\[NENA-STA-010.3\]](#). The Peering Network is responsible for their own QoS performance up to the VESTA NXT Router POI.

Security

VESTA NXT Router incorporates SBCs and Firewalls per NENA-STA-010.3.

Certificate establishment and key exchange algorithms must support PFS (Perfect Forward Secrecy). Upon establishing interconnection agreements VESTA NXT Router and Peering Network will establish security certificates issuing, deployment and agree upon renewal processes.

See the section above "[Transport Design](#)" for a discussion regarding VPN connection and SIPs and SRTP protocols.

All HTTP connections utilize HTTPS (HTTP/TLS (RFC 2818)).

DNS and IP Addressing

Both VESTA NXT Router and Peering Network are required to resolve URIs sent via SIP protocol and URLs sent via HTTPS protocol using DNS. VESTA NXT Router utilizes public IP addresses that are only routable over private dedicated connections and are not reachable from the Internet. VESTA NXT Router supports DNS SRV records and does not provide NAPTR records.

The Peering Network is required to provide its own DNS.

SIP Interface

This section describes the SIP Interface for Peering Networks interfacing to VESTA NXT Router. These statements generally apply to both OSPs and Neighbor i3 Routers except where specifically noted.

In a NENA i3 operating environment, OSPs deliver 9-1-1 calls to VESTA NXT Router via SIP messaging and provide HELD and ADR information services via HTTP (HTTPS) protocols.

VESTA NXT Router interacts with an Neighbor i3 Router for two purposes:

- Call hand-off with Neighbor i3 Router
- Call Transfer with an Neighbor i3 Router

VESTA NXT Router expects calls received from Neighbor i3 Router services SIP messages to include Call-Info headers with Call and Incident Identifiers. In addition it can, and should according to the NENA i3 specification, include History-Info headers specifying the routing of the call.

Common SIP Interface Requirements

This section applies to all i3 NNI Peering Network interfaces to VESTA NXT Router.

VESTA NXT Router implementation of SIP is based on RFC-3261 (SIP: Session Initiation Protocol) and RTP based on RFC-3550 (RTP: A Transport Protocol for Real-Time Applications).

SIP is expected to use the standard TCP port of 5060 (5061 for SIP over TLS). RTP will use a UDP port range determined by the Peering Network and agreed upon by VESTA NXT Router. Interfacing Peering Networks will see these SIP ports advertised from VESTA NXT Router SBCs.

SIP OPTIONS messaging is used to implement a heartbeat mechanism. SIP SUBSCRIBE/NOTIFY is also available to support a heartbeat mechanism.

SDP (Session Description Protocol) is utilized per NENA i3 specifications to negotiate media type and parameters.

VESTA NXT Router supports receiving a SIP 183 in response to a SIP INVITE. VESTA NXT Router will accept provisional ACKs (PRACK).

Calls presented to VESTA NXT Router must adhere to the following:

- Request URI must be urn:service:sos
- all telephone numbers must be signaled as a global TEL URI or a global SIP URI with parameter "user=phone"
- ESRP Queue must be identified in a Route header - topmost Route: header must specify the URI where the call is addressed. The Queue URI descriptors are mutually agreed upon between the VESTA NXT Router and Peering Networks for each supported call exchange scenario.
- INVITE must include a From header, if no P-A-I is provided then the From header MUST represent the callback number of the caller.
- INVITE may include a P-Asserted-Identity (P-A-I) header.
- INVITE must include at least one Geolocation header as defined in RFC6442. The Peering Network must provide a call location object in the SIP INVITE message either Location by Value (LbV) and/or Location by Reference (LbR).
- INVITE must include a Geolocation-Routing header as defined in RFC6442 with its value set to true.

VESTA NXT Router will utilize the first LbV presented in the SIP INVITE message to determine the call routing destination. If no LbV is present in the SIP INVITE message VESTA NXT Router will dereference the LbR. If no LbR or LbV is provided VESTA NXT Router will assign a default location based on the ESRP queue specified in the SIP Route header. If the queue cannot be resolved VESTA NXT Router will respond to the originating source with a SIP error message.

VESTA NXT Router will transport RTP Events (RFC-4733) between ingress and egress SIP interface entities (e.g., between Peering Networks and PSAP call route destinations). VESTA NXT Router will not detect embedded (e.g., in-band) RTP stream DTMF tones and will not transcribe in-band DTMF tones to RTP Events (RFC-4733).

SIP operations:

1. The i3 SIP calls to the ESRP can have Additional Data by Value or by Reference. If by Reference, the HTTPS URL must be reachable over the same IP interconnect points used to facilitate i3 SIP signaling and may be globally routable.
2. Elements ingressing calls shall allow configuration of the SIP Timer_B (Call Setup Time). Due to the emergency nature of provided call service, default SIP call timers are not satisfactory (i.e. users cannot wait 30 seconds for a ringtone.).
3. Elements ingressing calls shall support "SIP 302 Moved Temporarily" message according to RFC 3261.
4. Elements ingressing calls shall maintain the connection via heartbeat mechanism using SIP OPTIONS (during periods of inactivity).
5. Elements ingressing calls shall use SIP re-INVITE messages for SIP session keep-alive according to RFC 4028.
6. Elements ingressing calls will be provided with VESTA NXT Router FQDN which must be resolved using DNS SRV records when sending SIP requests/responses. Elements ingressing calls shall try each address found in SRV records until a VESTA NXT Router is contacted (according to RFC 3261 and RFC 3263).

RTT is supported upon request.

Calls Delivered to VESTA NXT Router Service for Routing

A Peering Network, an OSP or a Neighbor i3 Router, can send VESTA NXT Router a call that VESTA NXT Router is to route via NENA i3 algorithms. In addition to the common SIP operations described above, the following SIP message operations apply:

- INVITE must include a Call-Info: header of purpose EmergencyCallData.ProviderInfo as defined in RFC7852.
- INVITE must include a Call-Info: header of purpose EmergencyCallData.ServiceInfo as defined in RFC7852.
- INVITE may include a Call-Info: header of purpose EmergencyCallData.SubscriberInfo as defined in RFC7852 if information is known.

The INVITE Request header will be specific to a queue URI name provided by VESTA NXT Router. This queue name will indicate a geographic area to VESTA NXT Router and does not correspond to a specific PSAP URI.

Call Hand-off with Neighbor i3 Router

Call Hand-off scenarios are when a call is received at one 9-1-1 call router and that 9-1-1 call router determines the call needs to be delivered to another 9-1-1 call router. The first (originating) 9-1-1 call router delivers the call to a second (receiving) 9-1-1 call router with the expectation that the receiving 9-1-1 call router will “route” the call. As compared to a transfer scenario, the originating 9-1-1 call router does not identify the destination PSAP, rather the receiving 9-1-1 call router inspects the location information and determines the call destination. The section above, [“Calls Delivered to VESTA NXT Router Service for Routing”](#) applies to call hand-off scenarios.

VESTA NXT Router can perform the function of either the originating 9-1-1 call router or the receiving 9-1-1 call router. Call Hand-off scenarios, to or from VESTA NXT Router, are to include Geolocation headers as would be provided by an initial OSP ingress SIP INVITE message.

For 9-1-1 call hand-off scenarios, each upstream entity, VESTA NXT Router or the Neighbor i3 Router, will expose a LIS function (for HELD transactions) and ADR to the other 9-1-1 call routing entity as appropriate to the 9-1-1 call type (LbV or LbR).

There is no EIDO structure provided in a call hand-off scenario. EIDO is not relevant in 9-1-1 call router to 9-1-1 call router hand-off scenarios since an EIDO service is created by an originating PSAP CHE during a call transfer scenario.

VESTA NXT Router expects Neighbor i3 Router service SIP messages to include Call-Info headers with Call and Incident Identifiers. In addition it can include History-Info headers specifying the routing of the call.

Call Hand-off is a function needed for legacy OSP split wirecenter scenarios. The need to hand-off a call from one 9-1-1 call router to another 9-1-1 call router can occur with i3 OSPs, however, it is expected that i3

OSPs would properly deliver their 9-1-1 calls to the appropriate 9-1-1 call router service provider for the served area and corresponding PSAP jurisdiction.

Neighbor Call Router - Call Loop Prevention

VESTA NXT Router implements a call loop detection mechanism to determine if a call is received from a Neighbor i3 Router and VESTA NXT Router had previously directed the same call to the same Neighbor i3 Router. VESTA NXT Router will not route the call to the same Neighbor router again.

The connection between two 9-1-1 call routers creates the possibility of a call being routed by each call router to the other call router in a progressive fashion. In this scenario, each 9-1-1 call router determines, through its routing rules or “policies”, that the call is to “Hand-off” to the neighbor 9-1-1 call router, resulting in a “Loop” where the call is progressively presented by one call router to the other call router.

It is expected that every 9-1-1 call router will detect and prevent call loop scenarios. To prevent call Loop scenario, VESTA NXT Router requires, as is standard SIP behavior, that the neighbor 9-1-1 call router preserve previous “History-Info” headers. Each 9-1-1 call router is to preserve all “History-info” headers inserted by previous call processing entities. Each call router must inspect History-info headers and determine whether it has previously routed this call, and if so, perform a different call route action versus routing the call back to the same destination again.

Neighbor i3 Router Interactions - Call Transfer

The previous section for call hand-off, e.g., VESTA NXT Router receiving a call for routing, addresses some of the VESTA NXT Router interactions with a Neighbor i3 Router. This section addresses call transfer scenarios with a Neighbor i3 Router.

A Call transfer scenario is determined by the originating 9-1-1 call router specifying the destination PSAP by providing the PSAP’s URI in the SIP INVITE message Route header. VESTA NXT Router can initiate a PSAP to PSAP call transfer to a Neighbor i3 Router or can receive a PSAP to PSAP call transfer from a Neighbor i3 Router. The PSAP URIs must be mutually agreed upon between the two 9-1-1 call router providers.

Either 9-1-1 call router, VESTA NXT Router or the Neighbor i3 Router, can perform media bridge functions independent of the other entity. There is no visibility of a call bridge (conference) function between the 9-1-1 call router operating environments. VESTA NXT Router does not support Conference Event Package Subscribe/Notify functions with a Neighbor i3 Router.

Per NENA i3 standard, PSAP to PSAP 9-1-1 transfer calls are expected to specify an Emergency Incident Data Object (EIDO) URL provided by the originating PSAP and delivered to the destination PSAP. VESTA NXT Router will pass EIDO URLs provided by a Neighbor i3 Router (or the VESTA NXT Router proxied equivalent)

to the target VESTA NXT Router interconnected PSAP CHE. VESTA NXT Router will also pass EIDO URLs (or the VESTA NXT Router proxied equivalent) embedded in a SIP message from a VESTA NXT Router PSAP to the transfer destination PSAP of a Neighbor i3 Router.

As an interim approach in cases where EIDO exchange is not yet supported and upon mutual agreement with a Neighbor i3 Router, VESTA NXT Router will support transfer of calls using LIS/HELD and ADR as a means to transfer information in Neighbor i3 Router call transfer scenarios. In such scenarios, VESTA NXT Router will deliver the location information as received from the OSP to the Neighbor i3 Router (e.g., LbV and/or LbR). If originally a LbR OSP call, VESTA NXT Router will also deliver the location retrieved by VESTA NXT Router routing as LbV in addition to a LbR URL. ADR information will be conveyed to the Neighbor i3 Router as it was received by VESTA NXT Router (by value or by reference).

The network configuration for PSAP CHE to access an EIDO web service on a Neighbor i3 Router provider's network is currently not addressed within this document. The network engineering and IP path design to allow PSAPs in one 9-1-1 call router domain to access EIDO provided by a PSAP in another 9-1-1 call router domain is to be completed by mutual agreement with the entity requesting interconnection to VESTA NXT Router.

SIP INVITE message for call transfer scenarios with an Neighbor i3 Router:

- INVITE must include a Call-Info: header of purpose emergency-CallId as specified in section 3.1.6 of the NENA i3 standard.
- INVITE must include a Call-Info: header of purpose emergency-IncidentId as specified in section 3.1.7 of the NENA i3 standard.
- INVITE must include a Call-Info: header of purpose emergency-eido

SIP Headers

This section addresses SIP Headers used in various scenarios. Unrecognized SIP headers will be ignored.

Header	i3 SIP	Reference	Details
Accept	Optional	RFC 3261 Section 20.1	Example: Allow: INVITE, ACK, OPTIONS, PRAC, BYE

Allow	Required in SIP INVITE	RFC 3261 Section 20.5	Shall be present in the initial INVITE and its associated 200-OK response. Example: Allow: INVITE, ACK, OPTIONS, PRAC, BYE
Call-ID	Mandatory	RFC 3261 Section 20.8	
Call-Info	Mandatory	RFC 3261 Section 20.8	Must include NENA Call Tracking and Incident Identifiers and additional data about the call and caller and when the call is a transfer from a PSAP, a reference to an Emergency Incident Data Object (EIDO).
Contact	Mandatory	RFC 3261 Section 20.10	If the originator of the call is capable of processing conference-related REFER requests then "isfocus" parameter must be specified. The Parties will mutually agree upon implementation of this i3 SIP function.
Content-Length	Conditional	RFC 3261 Section 20.14	Must be present if there is a SIP body.
Content-Type	Conditional	RFC 3261 Section 20.15	Must be present if there is a SIP body with a MIME type. Example: Content-Type: multipart/mixed; boundary=boundary1
CSEQ	Mandatory	RFC 3261 Section 20.16	
From	Mandatory	RFC 3261 Section 20.20 Section 19.1.6	Contains the 9-1-1 caller's call back number. If a tel URL or SIP URI with parameter user=phone is provided, the phone number must comply to RFC-3966. Examples: From:<sip:+13125551234@carrier.example.com;user=phone>;tag=171828

			From:<tel:3125551234>;tag=171828
Geolocation	Mandatory	RFC 6442 Section 4.1	Provides location by value or by reference. The Geolocation header will either contain a location reference URI, or it will contain a Content-ID (CID) that points to the location in the message body where the location value is found. For LbR, the ESInet supports HTTP and HTTPS as pointers to the Location Object.
Geolocation-Routing	Mandatory	RFC 6442 Section 4.2	Define if location can be used for routing and could be set to yes or no. Must be set to yes for all calls delivered for routing. Location information used for routing is either LbV or LbR and correlates to the Geolocation header.
History-Info	Passthrough	RFC 4244	History-Info headers are passed through if received from a Neighbor i3 Router.
Max-Forwards	Mandatory	RFC 3261 Section 20.22	Example: Max-Forwards: 70
P-Access-Network-Info	Passthrough	RFC 3455	May indicate cell site. Example: P-Access-Network-Info:3GPP-E-UTRAN-FDD ;utran-cell-id-3gpp=0AE212345608A41F9
P-Asserted-Identity	Conditional	RFC 3325	The P-Asserted-Identity must represent the TN, MDN, or MSISDN of the caller that can be used to call the caller back. If a tel URL or SIP URI with parameter user=phone is provided, the phone number must comply with RFC-3966. Multiple PAI headers are acceptable.

			Example: P-Asserted-Identity:<tel:+13125551234> P-Asserted-Identity:<sip:+13125551234@carrier.example.net;user=phone>
P-ChargingVector	Passthrough	RFC 3455	May identify the originating carrier. Example: P-Charging-Vector:icid=34c23c445902;idid-generatedat=ecscf.carrier.example.net;orig-ioi=carrier.example.net
P-PreferredIdentity	Passthrough	RFC 3325	Example: P-Preferred-Identity:<sip:+13125551234@carrier.example.net;user=phone>
Record-Route	Optional	RFC 3261 Section 20.30	Example: Record-Route:<sip:sbc.carrier.example.com;lr>
Referred-By	Optional	RFC 3892	This header contains a URI of the PSAP which initiated a call transfer
Resource-Priority	Optional	RFC 4412 Section 3.1.7	This is a value from the “esnet” namespace according to i3 standard
Route	Mandatory	RFC 3261 Section 20.34	The top-most Route header must contain the target VESTA NXT Router ESRP queue URI. This value will be mutually agreed to between the call origination source and VESTA NXT Router for the given 9-1-1 Jurisdictional area. For Neighbor i3 Router handoff scenarios, the Route header is a predetermined generic URI and for call transfer scenarios it specifies the target PSAP.
Supported	Optional	RFC 3261 RFC 6442 Section 20.37	Example: geolocation-http per IANA: option tag is a string that is associated with a particular SIP option (that is, an extension).

			https://www.iana.org/assignments/sip-parameters/sip-parameters.xhtml#sip-parameters-4
To	Mandatory	RFC 3261 Section 20.39	Specifies a recipient of a SIP request
Unsupported	Optional	RFC 3261 Section 20.40	Example: Unsupported: 100rel
Via	Mandatory	RFC 3261 Section 20.42	Example: Via:SIP/2.0/UDP[aaa:bbb:ccc:ddd]:1357;branch=z9hG4bKnashds7

Media Interface

If SDP includes media-type specification for audio and/or video and/or RTT, then RTP media is exchanged. If SDP includes media-type specification for MSRP, then MSRP messages are exchanged.

RTP

VESTA NXT Router only supports G.711 uLaw codec with a 20ms packetization rate. It is expected that interconnecting networks not use silence suppression.

Media interface shall use RTP protocol (RFC 3550) over UDP. Note:

VESTA NXT Router implements a call disconnect (session termination) function upon Loss of RTP (> 30 seconds).

MSRP

The media type for Text-to-911 calls is MSRP. MSRP utilizes TCP as the transport protocol. All previous SIP messages and interaction description apply specific to VESTA NXT Router receiving 9-1-1 calls or Neighbor i3 Router interactions.

RTT

The media type and interaction models for Real Time Text (RTT) 9-1-1 calls. RTT will be documented in a future NNI specification version.

HELD & HTTPs Additional Data Interfaces

VESTA NXT Router supports HELD transactions to retrieve location information and HTTPs to retrieve additional data (ADR) from the origination call source.

Currently, for the geodetic location information shapes supported by VESTA NXT Router are:

- Point (2D-3D)
- Circle (2D)
- Ellipsoid (3D)

VESTA NXT Router requests that OSPs send location and ADR information by value, and by reference if the information is subject to change.

Supported SIP Error Codes

The following SIP error codes can be returned by VESTA NXT Router to the originating SIP entity (e.g., Peering Network).

SIP Error Code	Description
400	Bad Request
404	Not Found
405	Method Not Allowed
406	Not Acceptable
422	Session Interval Too Small
423	Interval Too Brief
483	Too Many Hops
481	Call/Transaction Does Not Exist
482	Loop Detected
483	Too Many Hops
484	Address Incomplete
486	Busy Here

487	Request Terminated
488	Not Acceptable Here
489	Bad Event
491	Request Pending
500	Internal Server Error
501	Not Implemented
504	Server Time-out
600	Busy Everywhere
604	Does Not Exist Anywhere

Examples

These messages are provided as examples (some of the additional data examples are coming from RFC-7852) and the implementations may not contain all fields described in those examples. One example of where this note is applicable is the vcard schema.

[Incoming] INVITE for a fixed location 9-1-1 call - LbV

```

INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/TCP 172.25.96.107;branch=z9hG4bK-393733-390f0759823370ed0a16f6d2f077fa38;rport
From: <sip:+17854140133@172.25.96.107>;tag=f5503a68-9454-402e-8ff8-1178813fa532
To: <sip:primary@esrp.msi-ngcs.com>
Call-ID: bfe0a7fe-9ff9-49bd-84ac-0cb17f38da75@172.25.96.107
CSeq: 1 INVITE
Contact: <sip:7854140133@172.25.96.107;transport=tcp>
Max-Forwards: 70
P-Access-Network-Info:
3GPP-UTRAN-FDD;local-time-zone="2017-09-02T10:15:31-31:00";utran-cell-id-3gpp=311480123400VESTA
P-Asserted-Identity: <sip:+17854140133@internal.msdevnet.com>
Content-Type: multipart/mixed;boundary="94c83325-f062-468e-9bb5-4093cf9e4ad5"
Content-Length: 4235
Call-Info: <urn:emergency:uid:incidentid:1733843012187-1974300153:example.com>;purpose=emergency-IncidentId
Call-Info: <urn:emergency:uid:callid:1733843012187-1532260243:example.com>;purpose=emergency-CallId
History-Info:
<sip:primary@esrp.msi-ngcs.com?Reason=emergency%3Bcause%3D200%3Btext%3D%22Normal%20Next%20Hop%22>;index=1
Geolocation: <cid:081694c1-054c-4428-9138-ee2e7aa87d6f@example.com>
Geolocation-Routing: yes
Route: <sip:primary@esrp.msi-ngcs.com;lr;transport=tcp>
User-Agent: MGS

Content-Type: application/pidf+xml
Content-Id: <081694c1-054c-4428-9138-ee2e7aa87d6f@example.com>

<?xml version="1.0" encoding="utf-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
entity="http://131.197.10.8/held/0d9bcae4-3f08-41ab-a203-f2160c8b9280">
  <tuple id="1526b2d0-0383-46ab-987e-63ed7615b57b">

```

© 2020-2025 Motorola Solutions Connectivity, Inc. and Motorola Solutions Connectivity of Virginia, Inc., wholly owned subsidiaries of Motorola Solutions, Inc. This document is protected by copyright law and international treaties, and is the CONFIDENTIAL AND PROPRIETARY information of Motorola Solutions Connectivity, Inc. All trademarks, service marks, product names, brands, company names and logos appearing in this document are the property of their respective owners. VESTA® is a registered trademark of Motorola Solutions Connectivity, Inc.

© 2020-2025, Motorola Solutions. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

```

<status>
  <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
    <location-info>
      <civicAddress xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
        <country>US</country>
        <A1>WV</A1>
        <A2>037</A2>
        <A3>KEARNEYSVILLE</A3>
        <RD>INDUSTRIAL</RD>
        <STS>BLVD</STS>
        <HNO>600</HNO>
        <NAM>JOE BOXCUTTER</NAM>
        <COMM xmlns="http://ddti.net/lostext">KEARNEYSVILLE</COMM>
        <ESN xmlns="http://911datamaster.com/pidfloext">99999</ESN>
      </civicAddress>
    </location-info>
    <usage-rules xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy">
      <retransmission-allowed>false</retransmission-allowed>
      <retention-expiry>2023-11-16T10:54:26.7818621-08:00</retention-expiry>
    </usage-rules>
    <method>Manual</method>
    <provided-by xmlns="urn:ietf:params:xml:ns:EmergencyCallData">
      <EmergencyCallDataValue>
        <EmergencyCallData.ProviderInfo xmlns="urn:ietf:params:xml:ns:EmergencyCallData:ProviderInfo">
          <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
          <ProviderID>urn:nena:companyid:TEST</ProviderID>
          <ProviderIDSeries>NENA</ProviderIDSeries>
          <TypeOfProvider>Telecom Provider</TypeOfProvider>
        </EmergencyCallData.ProviderInfo>
        <EmergencyCallData.ServiceInfo xmlns="urn:ietf:params:xml:ns:EmergencyCallData:ServiceInfo">
          <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
          <ServiceEnvironment>Business</ServiceEnvironment>
          <ServiceType>POTS</ServiceType>
          <ServiceMobility>Fixed</ServiceMobility>
          <LegacyClassOfService xmlns="http://ddti.net/addcallinfo" type="1">WPH1</LegacyClassOfService>
        </EmergencyCallData.ServiceInfo>
        <EmergencyCallData.DeviceInfo xmlns="urn:ietf:params:xml:ns:EmergencyCallData:DeviceInfo">
          <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
        </EmergencyCallData.DeviceInfo>
        <EmergencyCallData.SubscriberInfo xmlns="urn:ietf:params:xml:ns:EmergencyCallData:SubscriberInfo">
          <EmergencyCallData.Comment xmlns="urn:ietf:params:xml:ns:EmergencyCallData:Comment">
            <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
          </EmergencyCallData.Comment>
        </EmergencyCallData.SubscriberInfo>
      </EmergencyCallDataValue>
    </provided-by>
  </geopriv>
</status>
<timestamp>2023-11-16T10:53:26.7825107-08:00</timestamp>
</tuple>
</presence>

--94c83325-f062-468e-9bb5-4093cf9e4ad5
Content-Type: application/sdp

v=0
o=- 1733848553254 1733848553254 IN IP4 172.25.96.107
s=Media Server
t=0 0
m=audio 33262 RTP/AVP 0
c=IN IP4 172.25.96.107
a=rtcp:33263 IN IP4 172.25.96.107
a=sendrecv

--94c83325-f062-468e-9bb5-4093cf9e4ad5--

```


[Incoming] INVITE for an ATIS-0700015 Wireless Call - LbV and LbR

```

INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/TCP 172.25.96.107;branch=z9hG4bK-393733-390f0759823370ed0a16f6d2f077fa38;rport
From: <sip:+17854140133@172.25.96.107>;tag=f5503a68-9454-402e-8ff8-1178813fa532
To: <sip:primary@esrp.msi-ngcs.com>
Call-ID: bfe0a7fe-9ff9-49bd-84ac-0cb17f38da75@172.25.96.107
CSeq: 1 INVITE
Contact: <sip:7854140133@172.25.96.107;transport=tcp>
Max-Forwards: 70
P-Access-Network-Info:
3GPP-UTRAN-FDD;local-time-zone="2017-09-02T10:15:31-31:00";utran-cell-id-3gpp=311480123400VESTA
P-Asserted-Identity: <sip:7854140133@internal.msdevnet.com>
Content-Type: multipart/mixed;boundary="94c83325-f062-468e-9bb5-4093cf9e4ad5"
Content-Length: 5566
Call-Info: <urn:emergency:uid:incidentid:1733843012187-1974300153:example.com>;purpose=emergency-IncidentId
Call-Info: <urn:emergency:uid:callid:1733843012187-1532260243:example.com>;purpose=emergency-CallId
Call-Info: <cid:f968b79d-25ed-49ea-847b-4e0661cf275d@example.com>; purpose=EmergencyCallData.ServiceInfo,
<cid:4b894167-a85e-46f2-b846-50760626b93c@example.com>; purpose=EmergencyCallData.ProviderInfo
Geolocation: <https://held.example.com/9872394872-2342-2342>;purpose=heldDeref,
<cid:081694c1-054c-4428-9138-ee2e7aa87d6f@example.com>
History-Info:
<sip:primary@esrp.msi-ngcs.com?Reason=emergency%3Bcause%3D200%3Btext%3D%22Normal%20Next%20Hop%22>;index=1
Geolocation-Routing: yes
Route: <sip:primary@esrp.msi-ngcs.com;lr;transport=tcp>
User-Agent: MGS

--94c83325-f062-468e-9bb5-4093cf9e4ad5
Content-Type: application/EmergencyCallData.ServiceInfo+xml
Content-Id: <f968b79d-25ed-49ea-847b-4e0661cf275d@example.com>

<?xml version="1.0" encoding="UTF-8"?>
<svc:EmergencyCallData.ServiceInfo xmlns:svc="urn:ietf:params:xml:ns:EmergencyCallData:ServiceInfo">
<svc:DataProviderReference>2468.IBOC.MLTS.1359@example.org</svc:DataProviderReference>
<svc:ServiceType>Wireless</svc:ServiceType>
<svc:ServiceMobility>Mobile</svc:ServiceMobility>
</svc:EmergencyCallData.ServiceInfo>

--94c83325-f062-468e-9bb5-4093cf9e4ad5
Content-Type: application/EmergencyCallData.ProviderInfo+xml
Content-Id: <4b894167-a85e-46f2-b846-50760626b93c@example.com>

<?xml version="1.0" encoding="UTF-8"?>
<ad:EmergencyCallData.ProviderInfo xmlns:ad="urn:ietf:params:xml:ns:EmergencyCallData:ProviderInfo">
<ad:DataProviderReference>string0987654321@example.org</ad:DataProviderReference>
<ad:DataProviderString>Example VoIP Provider</ad:DataProviderString>
<ad:ProviderID>urn:nena:companyid:ID123</ad:ProviderID>
<ad:ProviderIDSeries>NENA</ad:ProviderIDSeries>
<ad:TypeOfProvider>Emergency Service Provider</ad:TypeOfProvider>
<ad:ContactURI>tel:+1-201-555-0123</ad:ContactURI>
<ad:Language>en</ad:Language>
</ad:EmergencyCallData.ProviderInfo>

--94c83325-f062-468e-9bb5-4093cf9e4ad5
Content-Type: application/pdf+xml
Content-Id: <081694c1-054c-4428-9138-ee2e7aa87d6f@example.com>

<?xml version="1.0" encoding="utf-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pdf">
entity="http://131.197.10.8/held/0d9bcae4-3f08-41ab-a203-f2160c8b9280">
<tuple id="1526b2d0-0383-46ab-987e-63ed7615b57b">
<status>
<geopriv xmlns="urn:ietf:params:xml:ns:pdf:geopriv10">
<location-info>
<Point xmlns="http://www.opengis.net/gml" srsName="urn:ogc:def:crs:EPSG::4326">
<pos>34.2215 -92.0019</pos>
</Point>
<civicAddress xmlns="urn:ietf:params:xml:ns:pdf:geopriv10:civicAddr">
<country>US</country>
<A1>AR</A1>

```

```

    <A2>Pine Bluff Public Library</A2>
    <A3>Pine Bluff</A3>
    <RD>S Main St</RD>
    <HNO>600</HNO>
    <NAM>7854140133</NAM>
    <COMM xmlns="http://ddti.net/lostext">Pine Bluff</COMM>
    <ESN xmlns="http://911datamaster.com/pidfloext">00000</ESN>
  </civicAddress>
</location-info>
<usage-rules xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy">
  <retransmission-allowed>false</retransmission-allowed>
  <retention-expiry>2023-11-16T10:54:26.7818621-08:00</retention-expiry>
</usage-rules>
<method>Manual</method>
<provided-by xmlns="urn:ietf:params:xml:ns:EmergencyCallData">
  <EmergencyCallDataValue>
    <EmergencyCallData.ProviderInfo xmlns="urn:ietf:params:xml:ns:EmergencyCallData:ProviderInfo">
      <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
      <ProviderID>urn:nena:companyid:TEST</ProviderID>
      <ProviderIDSeries>NENA</ProviderIDSeries>
      <TypeOfProvider>Telecom Provider</TypeOfProvider>
    </EmergencyCallData.ProviderInfo>
    <EmergencyCallData.ServiceInfo xmlns="urn:ietf:params:xml:ns:EmergencyCallData:ServiceInfo">
      <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
      <ServiceEnvironment>Business</ServiceEnvironment>
      <ServiceType>WIRELESS</ServiceType>
      <ServiceMobility>MOBILE</ServiceMobility>
      <LegacyClassOfService xmlns="http://ddti.net/addcallinfo" type="1">WPH1</LegacyClassOfService>
    </EmergencyCallData.ServiceInfo>
    <EmergencyCallData.DeviceInfo xmlns="urn:ietf:params:xml:ns:EmergencyCallData:DeviceInfo">
      <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
    </EmergencyCallData.DeviceInfo>
    <EmergencyCallData.SubscriberInfo xmlns="urn:ietf:params:xml:ns:EmergencyCallData:SubscriberInfo"
privacyRequested="false">
      <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
      <SubscriberData>
        <vcard xmlns="urn:ietf:params:xml:ns:vcard-4.0">
          <fn>
            <text>7854140133</text>
          </fn>
          <geo>
            <uri>geo:34.2215,-92.0019</uri>
          </geo>
          <tel>
            <uri>tel:7854140133</uri>
          </tel>
        </vcard>
      </SubscriberData>
    </EmergencyCallData.SubscriberInfo>
    <EmergencyCallData.Comment xmlns="urn:ietf:params:xml:ns:EmergencyCallData:Comment">
      <DataProviderReference>0d9bcae4-3f08-41ab-a203-f2160c8b9280</DataProviderReference>
    </EmergencyCallData.Comment>
  </EmergencyCallDataValue>
</provided-by>
</geopriv>
</status>
<timestamp>2023-11-16T10:53:26.7825107-08:00</timestamp>
</tuple>
</presence>

--94c83325-f062-468e-9bb5-4093cf9e4ad5
Content-Type: application/sdp

v=0
o=- 1733848553254 1733848553254 IN IP4 172.25.96.107
s= Media Server
t=0 0
m=audio 33262 RTP/AVP 0
c=IN IP4 172.25.96.107
a=rtcp:33263 IN IP4 172.25.96.107
a=sendrecv

```

--94c83325-f062-468e-9bb5-4093cf9e4ad5--

[Incoming] INVITE for an MSRP Text-to-911

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/TCP 172.25.96.107;branch=z9hG4bK-393733-390f0759823370ed0a16f6d2f077fa38;rport
From: <sip:+17854140133@172.25.96.107>;tag=f5503a68-9454-402e-8ff8-1178813fa532
To: <sip:primary@esrp.msi-ngcs.com>
Call-ID: bfe0a7fe-9ff9-49bd-84ac-0cb17f38da75@172.25.96.107
CSeq: 1 INVITE
Contact: <sip:7854140133@172.25.96.107;transport=tcp>
Max-Forwards: 70
P-Access-Network-Info:
3GPP-UTRAN-FDD;local-time-zone="2017-09-02T10:15:31-31:00";utran-cell-id-3gpp=311480123400VESTA
P-Asserted-Identity: <sip:7854140133@internal.msdevnet.com>
Content-Type: multipart/mixed;boundary="94c83325-f062-468e-9bb5-4093cf9e4ad5"
Content-Length: 195
Call-Info: <urn:emergency:uid:incidentid:1733843012187-1974300153:example.com>;purpose=emergency-IncidentId
Call-Info: <urn:emergency:uid:callid:1733843012187-1532260243:example.com>;purpose=emergency-CallId
History-Info:
<sip:primary@esrp.msi-ngcs.com?Reason=emergency%3Bcause%3D200%3Btext%3D%22Normal%20Next%20Hop%22>;index=1
Geolocation: <https://held.example.com/9872394872-2342-2342>;purpose=heldDeref
Geolocation-Routing: yes
Route: <sip:primary@esrp.msi-ngcs.com;lr;transport=tcp>
User-Agent: MGS
```

Content-Type: application/sdp

```
v=0
o=- 1728493043519 1 IN IP4 0.0.0.0
s=-
c=IN IP4 10.179.8.13
t=0 0
m=message 6002 TCP/MSRP *
a=accept-types:text/plain
a=setup:active
a=path:msrp://10.179.8.13:6002/Zf8mgnYpzLU;tcp
```

[Outgoing] INVITE for a Neighbor i3 Router - Call Hand-off

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/TCP 172.25.96.107;branch=z9hG4bK-393733-390f0759823370ed0a16f6d2f077fa38;rport
From: <sip:+17854140133@172.25.96.107>;tag=f5503a68-9454-402e-8ff8-1178813fa532
To: <sip:primary@esrp.example.com>
Route: <sip:primary@esrp.example.com;lr;transport=tcp>
Call-ID: bfe0a7fe-9ff9-49bd-84ac-0cb17f38da75@172.25.96.107
CSeq: 1 INVITE
Contact: <sip:7854140133@172.25.96.107;transport=tcp>
Max-Forwards: 70
P-Access-Network-Info:
3GPP-UTRAN-FDD;local-time-zone="2017-09-02T10:15:31-31:00";utran-cell-id-3gpp=311480123400VESTA
P-Asserted-Identity: <sip:7854140133@internal.msdevnet.com>
Content-Type: multipart/mixed;boundary="94c83325-f062-468e-9bb5-4093cf9e4ad5"
Content-Length: 195
History-Info:
<sip:primary@esrp.example.com?Reason=emergency%3Bcause%3D200%3Btext%3D%22Normal%20Next%20Hop%22>;index=1
Call-Info: <urn:emergency:uid:incidentid:1752837563455cot8k4staz4e:esrp.msi-ngcs.com>;purpose=emergency-IncidentId
Call-Info: <urn:emergency:uid:callid:17528375634557vgrhokv94fr:esrp.msi-ngcs.com>;purpose=emergency-CallId
Call-Info:
<https://proxy.msi-ngcs.com/ext?to=aHR0cHM6Ly9sZGIubXNpOTExLm5ldC9oZWxkL2FkZG10aW9uYWwEYXRhLzA5MDcxYTgyLTk0M2MtNGZi
MS04Y2JmLTJmNDQ2YWNlZTg4Ni9wcm92aWR1ckluZm8&sign=oxAXeoojeTbVYqBpuc-73K3Tet8QjrVlvjQzcX8V_8Mq7-cy6rTaV6-DSDP2vtzm6M
Totr5IdFayRj8a7pgXKq7OogfGDxroz6oOyw2dW1gKwI1lAwPuuHp_UxCVEGcNQvOZqoY9xAmGT55AelGBqHM55kRmA3pui5sq5pvXY8LCE-edhGO
QFjNPJRpb1E_Pfaw8DQDiA1-O8sB2_lbDYTxRmz80P6sqxzSomcTFPdtKv3IhM2FilpfxPGil-914BEy6jMxKLkiUqkUHDa7pv7ewP9QfyZNqdbQXL
7SD8t_UzzEcOEM2vqYyYAnu3GpgdcCeokor_tEd7H1SWAQ&id=1>;purpose=EmergencyCallData.ProviderInfo
Call-Info:
<https://proxy.msi-ngcs.com/ext?to=aHR0cHM6Ly9sZGIubXNpOTExLm5ldC9oZWxkL2FkZG10aW9uYWwEYXRhLzA5MDcxYTgyLTk0M2MtNGZi
MS04Y2JmLTJmNDQ2YWNlZTg4Ni9sZm92aWR1ckluZm8&sign=1hroxBVYgCZWM9zlu3mocuJMV6CyF1B3BvX8qJR-22KG0cXfDCqGIkOhB15er8AgN96
aLNTJPJ5xxzLzBhIA-9k-hnt4_Cc4waXmsrab9H40tCsbxxRt19W800h12I877nHgEuBPFNh21JWjO-mebW75KDgsv4oF23diKJ8F1pDJKgtLUQg9i9
```

© 2020-2025 Motorola Solutions Connectivity, Inc. and Motorola Solutions Connectivity of Virginia, Inc., wholly owned subsidiaries of Motorola Solutions, Inc. This document is protected by copyright law and international treaties, and is the CONFIDENTIAL AND PROPRIETARY information of Motorola Solutions Connectivity, Inc. All trademarks, service marks, product names, brands, company names and logos appearing in this document are the property of their respective owners. VESTA® is a registered trademark of Motorola Solutions Connectivity, Inc.

© 2020-2025, Motorola Solutions. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

```
sTPAE05M6iubecYxJXzk10s07J1vDSKx1ZyV0cZnswSxsha2IGjNZH4NZG30kAq2xnAzus7uyhHtM58yxf-9fj92hMgSVxuYfIO9hvlryuBVg9-H
emC1Pn7Hy_UIKPiR8XgNlFy3lalcViIcS8ZUzFk-YCuiqq&id=1>;purpose=EmergencyCallData.ServiceInfo
Call-Info:
<https://proxy.msi-ngcs.com/ext?to=aHR0cHM6Ly9sZGIubXNpOTExLm5ldC9oZWxkL2FkZG10aW9uYWwEYXRhLzA5MDcxYTgyLTk0M2MtNGZi
MS04Y2JmLTJvNDQ2YWNlZTg4Ni9kZkZpY2VJbmZv&sign=rSuFWLQzD9U-M8Yxfo2sffdNo3QHDu3jZkrFD20ej3LCKSEG_SGJegJuPCLQIonpwEC8
tJ6p-S1XrowguC7-U2Vy5klCKdad9oXt-JjCLxPv4aAYsQwfCxlTPBwp21plsN-clffKU58q2UqafP3e7rLEmjSSzP4KQqmf9Adw0JccFmHv7f9xACa
JbHh4oJZfFNHhhyOwtM2UGcEE8TROq0z4S5_O-b-s1wCVMA8F_ToCsFuUqacIt160P5DVNBXHLNKRd27QKnE-F1mY6d38fcyWMXhMct4ULW62UFRr
cON7kzU9RNHJRBJeB7Lk80J8vrYvR8U3vFB1gO7tA&id=1>;purpose=EmergencyCallData.DeviceInfo
Call-Info:
<https://proxy.msi-ngcs.com/ext?to=aHR0cHM6Ly9sZGIubXNpOTExLm5ldC9oZWxkL2FkZG10aW9uYWwEYXRhLzA5MDcxYTgyLTk0M2MtNGZi
MS04Y2JmLTJvNDQ2YWNlZTg4Ni9kZkZpY2VJbmZv&sign=YukI5Ple-Y5G9TFYZiezRzSI6f4WfsBHziYRUVm6-iW3nJCclo03pqa2xqzHQV0QT8rmFs-Ba
lZHVXEjDjnu53UrQMPeE3C5EMctAeu3RvYsIkfCXsHW3S4WntCeGjysJmQ8T9RvVWX0H_m8tjqCmHjlos2nPuETLnc-qSWK_5fnM5UYe0xe2bl8pYS
Oq_VyqYnOMV_NDrig5pUatDvzshCEoiKmwQlKHUT_PLc_9zYbhRO-HeHaIDK3Wvq42g0mkfbjKMrrITPr8CbiIMyq0bzmRGHSNcDHVhQLUp1b-8Elp
tTj81jKixLPchen12ZvZUmVbAu4jdZKopPUczg&id=1>;purpose=EmergencyCallData.Comment
Geolocation:
<https://proxy.msi-ngcs.com/ext?to=aHR0cHM6Ly9sZGIubXNpOTExLm5ldC9oZWxkL2FkZG10aW9uYWwEYXRhLzA5MDcxYTgyLTk0M2MtNGZi
MS04Y2JmLTJvNDQ2YWNlZTg4Ni9kZkZpY2VJbmZv&sign=YukI5Ple-Y5G9TFYZiezRzSI6f4WfsBHziYRUVm6-iW3nJCclo03pqa2xqzHQV0QT8rmFs-Ba
lZHVXEjDjnu53UrQMPeE3C5EMctAeu3RvYsIkfCXsHW3S4WntCeGjysJmQ8T9RvVWX0H_m8tjqCmHjlos2nPuETLnc-qSWK_5fnM5UYe0xe2bl8pYS
Oq_VyqYnOMV_NDrig5pUatDvzshCEoiKmwQlKHUT_PLc_9zYbhRO-HeHaIDK3Wvq42g0mkfbjKMrrITPr8CbiIMyq0bzmRGHSNcDHVhQLUp1b-8Elp
tTj81jKixLPchen12ZvZUmVbAu4jdZKopPUczg&id=1>;purpose=EmergencyCallData.Comment
Geolocation:
<https://proxy.msi-ngcs.com/ext?to=aHR0cHM6Ly9sZGIubXNpOTExLm5ldC9oZWxkL2FkZG10aW9uYWwEYXRhLzA5MDcxYTgyLTk0M2MtNGZi
MS04Y2JmLTJvNDQ2YWNlZTg4Ni9kZkZpY2VJbmZv&sign=YukI5Ple-Y5G9TFYZiezRzSI6f4WfsBHziYRUVm6-iW3nJCclo03pqa2xqzHQV0QT8rmFs-Ba
lZHVXEjDjnu53UrQMPeE3C5EMctAeu3RvYsIkfCXsHW3S4WntCeGjysJmQ8T9RvVWX0H_m8tjqCmHjlos2nPuETLnc-qSWK_5fnM5UYe0xe2bl8pYS
Oq_VyqYnOMV_NDrig5pUatDvzshCEoiKmwQlKHUT_PLc_9zYbhRO-HeHaIDK3Wvq42g0mkfbjKMrrITPr8CbiIMyq0bzmRGHSNcDHVhQLUp1b-8Elp
tTj81jKixLPchen12ZvZUmVbAu4jdZKopPUczg&id=1>;purpose=EmergencyCallData.Comment
User-Agent: MGS
```

Content-Type: application/sdp

```
v=0
o=CCMediaServer 508427017 2009960835 IN IP4 131.197.49.103
s=CCMediaServer
c=IN IP4 131.197.49.103
t=0 0
m=audio 24110 RTP/AVP 0 101
c=IN IP4 131.197.49.103
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtcp:24111
a=fmtp:101 0-15
```

[Outgoing] INVITE for a Neighbor i3 Router - PSAP Transfer

```
INVITE urn:service:sos SIP/2.0
Via: SIP/2.0/TCP 172.25.96.107;branch=z9hG4bK-393733-390f0759823370ed0a16f6d2f077fa38;rport
From: <sip:+17854140133@172.25.96.107>;tag=f5503a68-9454-402e-8ff8-1178813fa532
To: <sip:primary@esrp.example.com>
Route: <sip:primary@esrp.example.com;lr;transport=tcp>
Call-ID: bfe0a7fe-9ff9-49bd-84ac-0cb17f38da75@172.25.96.107
CSeq: 1 INVITE
Contact: <sip:7854140133@172.25.96.107;transport=tcp>
Max-Forwards: 70
P-Access-Network-Info:
3GPP-UTRAN-FDD;local-time-zone="2017-09-02T10:15:31-31:00";utran-cell-id-3gpp=311480123400VESTA
P-Asserted-Identity: <sip:7854140133@internal.msdevnet.com>
Content-Type: multipart/mixed;boundary="94c83325-f062-468e-9bb5-4093cf9e4ad5"
Content-Length: 195
Call-Info: <urn:emergency:uid:incidentid:1752837563455cot8k4staz4e:esrp.msi-ngcs.com>;purpose=emergency-IncidentId
Call-Info: <urn:emergency:uid:callid:17528375634557vgrhokv94fr:esrp.msi-ngcs.com>;purpose=emergency-CallId
Call-Info:
<https://proxy.msi-ngcs.com/ext?to=aHR0cDovL2lzaS1zaW1lbGF0aW9uLWVubHBvZG10aW9uYWwEYXRhLzA5MDcxYTgyLTk0M2MtNGZi
ZGFWc3henVyZS5jb20vaGVsZC9lC9xndWYyW50aW5lX2VpZG8&sign=RyEbxKqG1FtD3NqTodOqqJs804NAY0VELBK83Xilo1Q7ZvYNQGGq70x4Abc
mTt7WGOE3YADHNUKS3xR_JPSvAoxaca25L-se6J9Ij48T2DqVLW6T0W9X6bgkL0SZKHmTkj29gXyrBoxa_oYJVFRtxFuDCPIpDKqz58SWT63-Igda1
BVsDCwWSKykIvwUw_ahnIgJKMs6J7Qac-BZa-9eszyiC2T5AeoZ2TH0nndBN3v6cwE0H3wgnrcTwsF32G8wzh8zkLqarI8a5Ums24w3AD489UbiJ03m
Kaz3F14mNEVIFKc9reiE_Gqd_lXDelK2sVR8lom1Pxs214AD8B9GQw&id=1>;purpose=emergency-eido
```

Geolocation-Routing: yes
User-Agent: MGS

Content-Type: application/sdp

```
v=0
o=CCMediaServer 508427017 2009960835 IN IP4 131.197.49.103
s=CCMediaServer
c=IN IP4 131.197.49.103
t=0 0
m=audio 24110 RTP/AVP 0 101
c=IN IP4 131.197.49.103
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtcp:24111
a=fmtp:101 0-15
```

HELD locationResponse Example

```
<?xml version="1.0" encoding="utf-8"?>
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <presence xmlns="urn:ietf:params:xml:ns:pidf"
    entity="pres:3650n87934c@ls.example.com">
    <tuple id="b650sf789nd">
      <status>
        <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
          <location-info>
            <Point xmlns="http://www.opengis.net/gml" srsName="urn:ogc:def:crs:EPSG::4326">
              <pos>-34.407 150.88001</pos>
            </Point>
          </location-info>
          <usage-rules
            xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy">
            <gbp:retention-expiry>2024-09-11T03:42:28+00:00
            </gbp:retention-expiry>
          </usage-rules>
          <method>GPS</method>
        </geopriv>
      </status>
      <timestamp>2024-01-10T03:42:28+00:00</timestamp>
    </tuple>
  </presence>
</locationResponse>
```

ADR Response – Provider Info Example

```
<?xml version="1.0" encoding="UTF-8"?>
<ad:EmergencyCallData.ProviderInfo
  xmlns:ad="urn:ietf:params:xml:ns:EmergencyCallData:ProviderInfo">
  <ad:DataProviderReference>string0987654321@example.org
</ad:DataProviderReference>
  <ad:DataProviderString>Example VoIP Provider
</ad:DataProviderString>
  <ad:ProviderID>urn:nena:companyid:ID123</ad:ProviderID>
  <ad:ProviderIDSeries>NENA</ad:ProviderIDSeries>
  <ad:TypeOfProvider>Telecom Provider</ad:TypeOfProvider>
  <ad:ContactURI>tel:+1-201-555-0123</ad:ContactURI>
  <ad:Language>en</ad:Language>
  <ad:DataProviderContact
```

```

xmlns="urn:ietf:params:xml:ns:vcard-4.0">
  <vcard>
    <fn><text>Hannes Tschofenig</text></fn>
    <n>
      <surname>Hannes</surname>
      <given>Tschofenig</given>
      <additional/>
      <prefix/>
      <suffix>Dipl. Ing.</suffix>
    </n>
    <bday><date>--0203</date></bday>
    <anniversary>
      <date-time>20090808T1430-0500</date-time>
    </anniversary>
    <gender><sex>M</sex></gender>
    <lang>
      <parameters><pref><integer>1</integer></pref>
    </parameters>
    <language-tag>de</language-tag>
  </lang>
  <lang>
    <parameters><pref><integer>2</integer></pref>
  </parameters>
  <language-tag>en</language-tag>
</lang>
<org>
  <parameters><type><text>work</text></type>
</parameters>
  <text>Example VoIP Provider</text>
</org>
<adr>
  <parameters>
    <type><text>work</text></type>
    <label><text>Hannes Tschofenig
      Linnoitustie 6
      Espoo , Finland
      02600</text></label>
  </parameters>
  <pobox/>
  <ext/>
  <street>Linnoitustie 6</street>
  <locality>Espoo</locality>
  <region>Uusimaa</region>
  <code>02600</code>
  <country>Finland</country>
</adr>
<tel>
  <parameters>
    <type>
      <text>work</text>
      <text>voice</text>
    </type>
  </parameters>
  <uri>tel:+358 50 4871445</uri>
</tel>
<tel>
  <parameters>
    <type>
      <text>work</text>
      <text>main-number</text>

```

```

        <text>voice</text>
      </type>
    </parameters>
    <uri>tel:+358 50 5050505</uri>
  </tel>
  <email>
    <parameters><type><text>work</text></type>
    </parameters>
    <text>hannes.tschofenig@nsn.com</text>
  </email>
  <geo>
    <parameters><type><text>work</text></type>
    </parameters>
    <uri>geo:60.210796,24.812924</uri>
  </geo>
  <key>
    <parameters><type><text>home</text></type>
    </parameters>
    <uri>
      http://www.example.com/key.asc
    </uri>
  </key>
  <tz><text>Finland/Helsinki</text></tz>
  <url>
    <parameters><type><text>home</text></type>
    </parameters>
    <uri>http://www.tschofenig.priv.at</uri>
  </url>
</vcard>
</ad:DataProviderContact>
</ad:EmergencyCallData.ProviderInfo>

```

ADR Response – Service Info Example

```

<?xml version="1.0" encoding="UTF-8"?>
  <svc:EmergencyCallData.ServiceInfo
    xmlns:svc="urn:ietf:params:xml:ns:EmergencyCallData:ServiceInfo">
    <svc:DataProviderReference>lrf@osp.com
    </svc:DataProviderReference>
    <svc:ServiceEnvironment>Business</svc:ServiceEnvironment>
    <svc:ServiceType>POTS</svc:ServiceType>
    <svc:ServiceMobility>Fixed</svc:ServiceMobility>
  </svc:EmergencyCallData.ServiceInfo>

```

ADR Response – Device Info Example

```

<?xml version="1.0" encoding="UTF-8"?>
  <dev:EmergencyCallData.DeviceInfo
    xmlns:dev="urn:ietf:params:xml:ns:EmergencyCallData:DeviceInfo">
    <dev:DataProviderReference>d4b3072df.201409182208075@example.org
    </dev:DataProviderReference>
    <dev:DeviceClassification>fixed</dev:DeviceClassification>
    <dev:DeviceMfg>Nokia</dev:DeviceMfg>
    <dev:DeviceModelNr>Lumia 800</dev:DeviceModelNr>
    <dev:UniqueDeviceID TypeOfDeviceID="IMEI">35788104
    </dev:UniqueDeviceID>
  </dev:EmergencyCallData.DeviceInfo>

```

```
</dev:EmergencyCallData.DeviceInfo>
```

ADR Response – Comment Example

```
<?xml version="1.0" encoding="UTF-8"?>
  <com:EmergencyCallData.Comment
    xmlns:com="urn:ietf:params:xml:ns:EmergencyCallData:Comment">
    <com:DataProviderReference>string0987654321@example.org
  </com:DataProviderReference>
  <com:Comment xml:lang="en">This is an example text.</com:Comment>
</com:EmergencyCallData.Comment>
```

ADR Response – Subscriber Info Example

```
<?xml version="1.0" encoding="UTF-8"?>
  <sub:EmergencyCallData.SubscriberInfo
    xmlns:sub=
      "urn:ietf:params:xml:ns:EmergencyCallData:SubscriberInfo"
    privacyRequested="false">
    <sub:DataProviderReference>FEABFECD901@example.org
  </sub:DataProviderReference>
  <sub:SubscriberData xmlns="urn:ietf:params:xml:ns:vcard-4.0">
    <vcard>
      <fn><text>Simon Perreault</text></fn>
      <n>
        <surname>Perreault</surname>
        <given>Simon</given>
        <additional/>
        <prefix/>
        <suffix>ing. jr</suffix>
        <suffix>M.Sc.</suffix>
      </n>
      <bday><date>--0203</date></bday>
      <anniversary>
        <date-time>20090808T1430-0500</date-time>
      </anniversary>
      <gender><sex>M</sex></gender>
      <lang>
        <parameters><pref><integer>1</integer></pref>
      </parameters>
      <language-tag>fr</language-tag>
    </lang>
    <lang>
      <parameters><pref><integer>2</integer></pref>
    </parameters>
    <language-tag>en</language-tag>
  </lang>
  <org>
    <parameters><type><text>work</text></type>
  </parameters>
  <text>Viagenie</text>
</org>
  <adr>
    <parameters>
      <type><text>work</text></type>
      <label><text>Simon Perreault
```



```

                2875 boul. Laurier, suite D2-630
                Quebec, QC, Canada
                G1V 2M2</text></label>
</parameters>
<pobox/>
<ext/>
<street>2875 boul. Laurier,
        suite D2-630</street>
<locality>Quebec</locality>
<region>QC</region>
<code>G1V 2M2</code>
<country>Canada</country>
</adr>
<tel>
  <parameters>
    <type>
      <text>work</text>
      <text>voice</text>
    </type>
  </parameters>
  <uri>tel:+1-418-656-9254;ext=102</uri>
</tel>
<tel>
  <parameters>
    <type>
      <text>work</text>
      <text>voice</text>
      <text>main-number</text>
    </type>
  </parameters>
  <uri>tel:+1-418-555-0000</uri>
</tel>
<tel>
  <parameters>
    <type>
      <text>work</text>
      <text>text</text>
      <text>voice</text>
      <text>cell</text>
      <text>video</text>
    </type>
  </parameters>
  <uri>tel:+1-418-262-6501</uri>
</tel>
<email>
  <parameters><type><text>work</text></type>
</parameters>
  <text>simon.perreault@viagenie.ca</text>
</email>
<geo>
  <parameters><type><text>work</text></type>
</parameters>
  <uri>geo:46.766336,-71.28955</uri>
</geo>
<key>
  <parameters><type><text>work</text></type>
</parameters>
  <uri>
    http://www.viagenie.ca/simon.perreault/simon.asc
  </uri>

```

```

        </key>
        <tz><text>America/Montreal</text></tz>
        <url>
            <parameters><type><text>home</text></type>
            </parameters>
            <uri>http://nomis80.org</uri>
        </url>
    </vcard>
</sub:SubscriberData>
</sub:EmergencyCallData.SubscriberInfo>

```

MSRP Message

```

MSRP WIwI0imlTiPM SEND
To-Path: msrp://10.65.54.159:27000/k0h2E000;tcp
From-Path: msrp://131.197.49.105:5500/gJW86fptYz4dp;tcp
Message-ID: vUpVU0wcuKzt
Byte-Range: 1-15/15
Content-Type: text/plain text/x-msrp-heartbeat

```

Are you there?

-----WIwI0imlTiPM\$

MSRP Handshake Message

```

MSRP MgTqxKDJHeBjHT9i SEND
To-Path: msrp://10.65.54.159:27000/k0h2E000;tcp
From-Path: msrp://131.197.49.105:5500/gJW86fptYz4dp;tcp
Message-ID: AuL8T2TJRNdLlbJ
Byte-Range: 1-0/0
Content-Type: text/plain
-----MgTqxKDJHeBjHT9i$

```

Appendices

Reference Documents

- [NENA-STA-010.3](#) - Detailed Functional and Interface Specification for the NENA i3 Solution
- [ATIS-0700015](#) - ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination (document number)
- [NENA-INF-016.2-2018](#) - Emergency Services IP Network Design (ESIND) Information Document
- International Telecommunications Union (ITU) One-way Transmission Time ([G.114](#))

IETF RFC Standard References

[RFC-2475](#): An Architecture for Differentiated Services

[RFC-2818](#): HTTP Over TLS

[RFC-2833](#): RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

[RFC-3261](#): SIP: Session Initiation Protocol

[RFC-3262](#): Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

[RFC-3263](#): Session Initiation Protocol (SIP): Locating SIP Servers

[RFC-3264](#): An Offer/Answer Model with the Session Description Protocol (SDP)

[RFC-3311](#): The Session Initiation Protocol (SIP) UPDATE Method

[RFC-3323](#): A Privacy Mechanism for the Session Initiation Protocol (SIP)

[RFC-3325](#): Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

[RFC-3326](#): The Reason Header Field for the Session Initiation Protocol (SIP)

[RFC-3398](#): Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping

[RFC-3455](#): Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)

[RFC-3515](#): The Session Initiation Protocol (SIP) Refer Method

- [RFC-3525](#): Gateway Control Protocol Version 1
- [RFC-3550](#): RTP: A Transport Protocol for Real-Time Applications
- [RFC-3711](#): The Secure Real-time Transport Protocol (SRTP)
- [RFC-3761](#): The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
- [RFC-3824](#): Using E.164 numbers with the Session Initiation Protocol (SIP)
- [RFC-3891](#): The Session Initiation Protocol (SIP) "Replaces" Header
- [RFC-3966](#): The tel URI for Telephone Numbers
- [RFC-4028](#): Session Timers in the Session Initiation Protocol (SIP)
- [RFC-4033](#): DNS Security Introduction and Requirements
- [RFC-4034](#): Resource Records for the DNS Security Extensions
- [RFC-4035](#): Protocol Modifications for the DNS Security Extensions
- [RFC-4244](#): An Extension to the Session Initiation Protocol (SIP) for Request History Information
- [RFC-4317](#): Session Description Protocol (SDP) Offer/Answer Examples
- [RFC-4488](#): Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription
- [RFC-4566](#): SDP: Session Description Protocol
- [RFC-4694](#): Number Portability Parameters for the "tel" URI
- [RFC-4733](#): RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- [RFC-4904](#): Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)
- [RFC-5031](#): A Uniform Resource Name (URN) for Emergency and Other Well-Known Services
- [RFC-5923](#): Connection Reuse in the Session Initiation Protocol (SIP)
- [RFC-6442](#): Location Conveyance for the Session Initiation Protocol
- [RFC-6665](#): (Future) SIP-Specific Event Notification
- [RFC-6881](#): Best Current Practice for Communicating Services in Support of Emergency Calling

[RFC-7852](#): Additional Data Related to an Emergency Call

Exhibit 3 Prohibited Communications Equipment Affidavit

**AFFIDAVIT REGARDING THE USE OF
PROHIBITED COMMUNICATIONS EQUIPMENT**

STATE OF Arizona)
) ss:
COUNTY OF Maricopa)

NAME OF COMPANY: Motorola Solutions Connectivity, Inc.

AUTHORITY HELD IN NEBRASKA (check all that apply):

- ☐ Incumbent Local Exchange Carrier (ILEC)
- ☐ Competitive Local Exchange Carrier (CLEC)
- ☐ Interexchange Carrier (IXC)
- ☐ Eligible Telecommunications Company (ETC)
- ☒ Communications Provider

The undersigned affiant, upon first being duly sworn, does hereby depose and state:

I, Travis Boettcher, am a duly appointed representative or employee
of Motorola Solutions Connectivity Inc., and hold the position of CVP Software Sales.

I am familiar with the communications equipment currently in use and scheduled to be used in the foreseeable future by the above-listed company. I am also familiar with the Covered List of prohibited equipment maintained by the Federal Communications Commission and have reviewed the providers included on the Covered List as of the date of this Affidavit.

In preparation to complete this Affidavit, I have reviewed the communications equipment currently in use and scheduled to be used by the above-listed company. Based upon that review, and to the best of my knowledge and belief based upon all information available to me in my professional role with this company, I hereby attest that this company

☐ IS

☒ IS NOT

using or deploying communications equipment and services developed by organizations on the Federal Communications Commission's Covered List.

AFFIDAVIT REGARDING THE USE OF PROHIBITED EQUIPMENT

Company Name: Motorola Solutions Connectivity, Inc.

I understand that any failure to fully disclose the use or deployment of prohibited equipment in this affidavit may result in penalties against myself and/or the above-listed company.

I attest that should information come to my attention which would change my response listed above, I will report this information to the Nebraska Public Service Commission without delay.

I attest that I will ensure this form is completed on an annual basis by the above-listed company and submitted prior to April 30 of each year to the Nebraska Public Service Commission.

All foregoing acknowledgements and attestations in this affidavit are true and correct to the best of my information and belief.

[Signature], Affiant

Company Officer's Signature

→ **(Cannot be a 3rd Party Filer)**

Travis Boettcher

[Print Name of Affiant]

CVP Software Sales

[Affiant's Title]

Motorola Solutions Connectivity, Inc.

[Company Name]

500 W Monroe St. Ste 4400

[Company Address]

Chicago, IL 60661-3781

[Company City / State / Zip Code]

(480) 980-9579

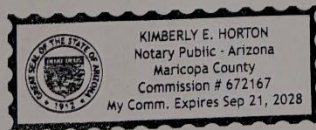
[Affiant's Telephone Number]

travisb@motorolasolutions.com

[Affiant's E-Mail Address]

Acknowledged, subscribed, and sworn to me on this 14th day of April, 2026.

(Affix Seal Here)



[Signature]
Notary Public

Exhibit 4 Sample Project Management Plan

State of Nebraska

Motorola Solutions Connectivity, Inc.

Sample Project Management Plan

Motorola Solutions Connectivity, Inc., is a wholly owned subsidiary of Motorola Solutions, Inc. This document is protected by copyright law and international treaties, and is the information of Motorola Solutions Connectivity, Inc. All trademarks, service marks, product names, brands, company names and logos appearing in this document are the property of their respective owners. VESTA® is a registered trademark of Motorola Solutions Connectivity, Inc.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2026 All rights reserved.

Table of Contents

Section 1 Project Management Plan.....	5
1.1. Project Management and Implementation Methodology.....	5
1.1.1. Project Team Staffing.....	6
Project Manager.....	6
NGCS Solutions Architect.....	7
Network Services Lead.....	7
Operations/Support/Service Manager.....	8
1.2. Schedule Management.....	8
1.3. Communications Plan.....	9
1.4. Action Items / Issues Management Plan.....	10
1.5. Change Management Plan.....	10
1.6. Risk Management Plan.....	11
1.7. Project Punch List.....	12
1.8. Quality Management Overview.....	13
1.8.1. Quality Assurance and Control.....	13
1.8.2. Quality Management Process.....	14
1.9. Governance Approach.....	15
Section 2 Project Implementation Plan.....	16
2.1.1. Detailed Design Review.....	16
2.1.2. NGCS Installation and Provisioning.....	17
Core Routing Functions.....	17
2.1.3. Ingress Network Implementation and Carrier Migration.....	19
2.1.4. Egress Network Implementation (ESInet).....	20
2.1.5. Location Database (LDB) Data Migration.....	21
Phase 1.....	21
Phase 2.....	21
Phase 3 (If Applicable).....	22
2.1.6. NGCS Data Provisioning.....	23
Section 3 PSAP Transition/Migration Plan.....	24
3.1. System Construction.....	25
3.1.1. NGCS Elements.....	25
3.1.2. ESInet Connectivity.....	25
3.1.3. PSAPs and Call Handling Host Elements.....	26
3.2. Carrier Migration, Ingress, and Egress Network Validation.....	27
3.2.1. Carrier Identification and Call Capacity Analyses.....	27
3.2.2. Ingress to the Call Routing Service.....	27

3.2.3. Migration and Validation.....	27
3.2.4. ESInet Connectivity and NGCS Egress Network Validation.....	28
3.3. Migration Planning.....	30
3.3.1. Acceptance Testing.....	30
3.3.2. Migration Plan.....	30
3.3.3. OSP and PSAP Migration to the New Routing Service.....	30
3.3.4. Legacy Selective Routers and ALI Data.....	36
Legacy Selective Routers.....	36
ALI Data.....	36
3.4. PSAP Migration.....	36
3.5. Text to 9-1-1.....	37
3.6. Interoperability.....	37
3.7. Migration Phases.....	37
3.7.1. Pre-Migration Tasks.....	37
3.7.2. Migration Tasks.....	39
3.7.3. Post-Migration Tasks.....	39
3.8. Project Finalization.....	40
Section 4 Training Structure.....	41
4.1.1. Training Methodology.....	41
4.2. Training Plan Statement of Work.....	41
4.2.1. Instructor Responsibilities.....	41
Training Implementation.....	41
Instruction and Facilitation.....	42
Closing Activities.....	42
4.3. State of Nebraska and PSAP Responsibilities.....	42
4.3.1. NGCS Routing Service & ESInet Overview.....	44
Description.....	44
4.3.2. NGCS GIS Tools and Procedures, Database Management Overview, Spatial Interface.....	44
4.3.3. NGCS Location Database (LDB) Management.....	45
4.3.4. Customer Web Portal.....	46
Section 5 Support Plans.....	48
5.1.1. NSOC and Service Management.....	48
5.1.2. NGCS i3 Event Logger.....	49
Section 6 PSAP Acceptance Test Plan.....	50
6.1. Purpose.....	50
6.1.1. Scope.....	50
6.2. Prerequisites.....	51
6.3. Demarcation Point Verification.....	51

6.3.1. ESInet Edge Router / Physical Connectivity.....	51
6.4. MSCI NGCS Service Configuration - Customer Specific.....	51
6.4.1. MSCI NGCS Configuration.....	51
6.4.2. Conference / Transfer Function.....	52
6.5. Pre-Test System Observations.....	52
6.6. Location Service Testing.....	52
6.7. Location Database Service Testing.....	53
6.8. Wireline Test Call.....	53
6.9. No Record Found Wireline Test Call.....	53
6.10. Wireless Test Call.....	54
6.11. 10-Digit PSTN Test Call.....	54
6.12. Conference Bridge and NGCS Transfer Testing.....	54
6.13. Ring No Answer Call Routing.....	54
6.14. Error Code Call Routing.....	55
6.15. Abandoned State Routing.....	55
Section 7 Project Finalization.....	56

Section 1

Project Management Plan

Motorola Solutions Connectivity, Inc. (MSCI) Project Management Plan provides the framework for successfully implementing the NG9-1-1 service based on MSCI's extensive experience in deploying complex, integrated public safety solutions. This plan will be further developed in partnership with the State of Nebraska and submitted as a formal plan as part of the project documentation during the Detailed Design Review. The Project Management Plan comprises the Project Management and Implementation Methodology, Project Implementation Plan, migration/migration planning, Acceptance Test Plan (ATP) objectives, and Training Plan.

It is understood that this is a working document that will be revised, as needed, to incorporate any changes associated with Detailed Design Review and any other changes that may occur during the execution of the project.

1.1. Project Management and Implementation Methodology

Our Project Manager will lead all necessary project team members in the implementation process by communicating the agreed-upon project plan, project status, identified risks, and next steps to their teams. Our Project Manager, working with the project team, is responsible for formulating the project plans required to implement the project, communicating the support plan for the service, and coordinating activities to ensure a successful go-live with minimal risk and disruption to the public safety answering point (PSAP). The project team will use a combined Project Management Plan (PMP) and Project Schedule ([Smartsheet](#) and [Project Dashboard](#)) to provide a consistent vehicle for communication, management, reporting of progress, and to address any potential progress delays.

This Project Management Plan includes a brief synopsis of the project management methodology related to overall program management components to deliver the contracted project on time and within budget. It includes the following components, which are further described in the sections below:

- Project Team Staffing
- Schedule Management
- Communications Plan
- Action Items / Issues Management Plan
- Change Management Process
- Risk Management Process

- Project Punch List
- Quality Management
- Governance Approach

Note: Links to the live Project Management Dashboard and Master Schedule will be activated upon contract execution. Once live, these resources will be accessible 24/7 to all authorized personnel.

1.1.1. Project Team Staffing

The project staff is a team of specialists that will form a cohesive working group with State of Nebraska's project staff. The project team is backed by MSCI product development, project management office, cybersecurity, and support organizations. All of these resources will be led by the Project Manager. Should the need arise for staffing changes, MSCI will work with the State of Nebraska to designate new resources and ensure that all personnel have the requisite skills and experience. Additional to the project team are suppliers of services within the NGCS solution, such as OSP migration and ESInet transport links. MSCI's portfolio of carefully selected suppliers and subcontractors will follow the same high-quality standards as we do through rigorous oversight of their work. The roles and responsibilities of key project team members are described further below.

The Responsible, Accountable, Consulted, and Informed (RACI) chart for this project clarifies roles and responsibilities and can be found in the [Project Dashboard](#).

Project Manager

The Project Manager will lead all project team meetings and manage contract terms, project schedule, communications plan, risk management, and quality assurance plans. The Project Manager will represent the sole authority for project actions and reporting and will be responsible for quality performance and cost control. They will enforce performance standards, control risks, and oversee resolution to technical issues throughout all implementation phases.

The Project Manager's responsibilities include:

- Continuously monitor the project's contractual obligations, milestones, deliverables, and customer satisfaction.
- Assume overall responsibility for scheduling project tasks and directing project resources. Maintain the project plan and schedule showing the entire project, including a Gantt Chart depicting the responsibilities of all relevant parties.
- Manage the Change Management process throughout project implementation.
- Prepare for and conduct design reviews, policy routing, and regular progress meetings and provide progress reports, as required.
- Document and communicate project progress to project stakeholders.
- Manage and document project acceptance testing.
- Obtain sign-off and acceptance upon completing the installation, acceptance testing, and training.

- Assume primary responsibility for migration coordination and support.
- Provide post-go-live issue documentation and resolution support.
- Conduct post-go-live evaluation and transition to ongoing support.
- Facilitate project finalization and closeout.

NGCS Solutions Architect

The lead NGCS Solutions Architect is responsible for overall system design, which accounts for the functional elements of the NGCS routing service, migration of Originating Service Providers, and the specification and deployment of the ESInet WAN connectivity design. Network Solutions Architects will supplement the lead Solutions Architect and support the implementation of ESInet connections and carrier migrations. The lead Solutions Architect will ensure the technical integrity of the NGCS design and will be supported by additional NGCS Solutions Architects, engineers and GIS professionals throughout the project. Under the lead Solutions Architect's leadership, the following tasks will be performed:

- Create and maintain the design, beginning with the contract design review, updating, and finalizing documentation throughout the implementation of the NGCS routing service.
- Serve as the NGCS technical point of contact and collaborate with product engineering, service, and support teams.
- Manage technical aspects of carrier migration, ESInet, and location services activities to ensure the integrity of the NGCS subsystem.
- Develop detailed design documentation reflecting the as-built network inclusive of NGCS and ESInet elements.
- Participate in the implementation, and perform the following tasks:
 - Develop configurations and program equipment.
 - Develop and participate in functional and operational ATPs.
- Assist in developing and performing the PSAP migration and go-live to the new NGCS platform.
- Provide continuous technical support throughout the project and after project acceptance.

Network Services Lead

A Network Services project lead will be assigned to work with selected carriers and State of Nebraska staff to ensure the scheduled rollout of circuits for the ESInet deployment meets the agreed-upon project schedule. Responsibilities include the following tasks:

- Serve as the single point of contact for all carriers during the ESInet deployment.
- Place orders for all circuits.
- Track circuit orders and obtain firm order completion (FOC) dates.
- Ensure IP transport elements are installed, turned up, and tested correctly.
- Work with the lead Solutions Architect to verify that the circuit/bandwidth meets engineering requirements.
- Work with Carriers to address any remediation efforts required to bring circuits online.

Operations/Support/Service Manager

An Operations Manager (Software Services Customer Manager/Customer Support Manager) is assigned to provide the State of Nebraska with a single point of contact and manage the contracted maintenance and support services. The Operations Manager works with the on-site support personnel and is backed by MSCI's service and support organization. The MSCI support organization includes the Network Security Operations Center (NSOC), Technical Support, and product management teams. All work in concert with field-based System Managers and on-site support personnel to deliver services and maintain Service Level Agreements.

The responsibilities include the following tasks:

- Create and maintain the Support Plan that is reflective of Support Services sold with the contract.
- Establish and refine policies and procedures to consistently maximize service performance.
- Proactively manage the life cycle of the service and supply information regarding upgrades and updates.
- Engage the appropriate resources, teams, and individuals to troubleshoot and resolve complex service issues.
- Serve as the escalation point of contact when standard troubleshooting efforts are unsuccessful.
- Serve as the liaison to MSCI's support organization for escalated incidents.
- Provide timely and frequent informational updates about progress toward resolving incidents.
- Ensures maintenance and performance quality of the system with the LOB/NGCS.
- Monitor MSCI's contractual performance / service level agreements (SLAs) and provide reviews and analyses of SLA performance metrics.
- Manage the Change Management process during the Service operation.

1.2. Schedule Management

Our Project Schedule will include all project work activities, responsibilities for performing those activities, and proper sequencing. The schedule will be maintained in Smartsheet and be accessible to State of Nebraska project team members.

The Project Schedule details the projected timeline for completing the tasks required to implement the new NG9-1-1 service successfully. During the Detailed Design Review meeting following the contract award, the Project Manager will present a baseline project schedule that will be mutually agreed upon based on knowledge and timeline goals learned during the initial project kick-off meeting.

The Project Manager will update the baseline schedule weekly during project implementation. A [Project Dashboard](#) using Google Sheets will supplement the schedule and help the Project Team visualize major aspects of the implementation. Real-time access to the Schedule is embedded within the Project Dashboard. MSCI will work with the State of Nebraska to identify all project responsibilities for successfully completing the project.

1.3. Communications Plan

MSCI recognizes that prompt and effective communication is vital to integrating project teams and completing projects and will collaborate to create a project Communications Plan during project initiation. The plan will:

- Define the communication process the teams will use throughout the project.
- Determine what communication tools the project team will use to send information and report on progress. Communication tools may include email, status reports, phone, fax, and websites.
- Ensure project success is measured accurately.
- Provide continuous access to status reports, schedules, and other key documents.
- Provide the field team with immediate, fast-track issue resolution information.
- Clearly identify the key project stakeholders and project team members.
- Avoid costly miscommunications.

The Project Manager will be responsible for scheduling and conducting meetings regularly to be determined and mutually agreed upon. This will include regular bi-weekly or weekly project status meetings, or as needed and agreed upon, throughout the project with team members from both parties. For every meeting, the Project Manager will provide mutually agreed upon agendas and project-specific materials at least 24 hours before the meeting and meeting notes within one (1) business day of meeting completion. The status meetings will typically cover the following topics and contain enough detail to enable stakeholders to make informed decisions and effectively oversee the project:

- Overall project status on major activities and key deliverables.
- Status of issues and action items with assignments.
- Project Schedule updates and review of future planned activities (to be distributed at least one (1) day before the scheduled meeting).
- Status of risk register items.

Regular project status reports will be posted by the Project Manager on a shared website, with access provided to the project community. Representatives of the State of Nebraska will be able to view the status of each site quickly, and the project team will be able to reference the schedule and project documentation progress readily.

Status reports will highlight potential issues and identify actions to mitigate them. Individual action items will be assigned, and the Project Manager will track completion dates. Status reports will also assess the project's progress and communicate resources. Action item lists will be maintained and updated weekly to identify and resolve identified items.

As the PSAP migration to the new NG9-1-1 service nears, status meetings and reports will be more frequent. MSCI's technical staff and Project Manager will be on-site during the migration. They will communicate with State of Nebraska's Project Manager and relevant PSAP personnel daily or as activity levels require.

1.4. Action Items / Issues Management Plan

The Project Management Plan includes developing an Action Items/Issues Management Plan that will be used throughout the project to resolve issues within the project's scope. Team members will determine if an issue that arises during the project, such as an unsatisfactory test result or unexpected problem, may significantly impact project completion and need to be reported to the Project Manager. The Project Manager will consult with the team member to determine the issue's impact and decide if it should be reported to the full project team.

To ensure the plan incorporates State of Nebraska's priorities, the Project Manager will work with State of Nebraska's Project Manager during the initiation phase to design and approve the Action Items/Issues Log format.

Issues that change or modify parts of the project scope, including product quantities, schedule, and deliverables, are handled through the Change Management process. The Action Items/Issues Log identifies issues, provides continual status updates on specific tasks and identifies the responsibilities of all parties.

1.5. Change Management Plan

MSCI uses a detailed, IT Information Library (ITIL)-based Change Management process to ensure standardized methods and procedures are followed for completing project changes efficiently and promptly. The Change Management process intends to ensure the State of Nebraska and MSCI agree on any documented and recorded contract baseline changes.

MSCI will maintain effective change management during the project implementation to capture the impact of any proposed changes to the requirements. We will collaborate with the State of Nebraska to determine the impact of any change request on scope, cost, and schedule; and will document the agreed-upon changes on the Change Control Order (CCO) form. Any resulting change order must be authorized and executed by the State of Nebraska and MSCI before work on the change order can begin.

During service delivery, we use the Change Management process to avoid or minimize the impact of change-related incidents and prevent disruption to day-to-day operations.

The Change Management process ensures that service change requests are properly documented, reviewed, and approved by stakeholders before implementation. The Change Management process will be defined and documented in detail during the project planning phase. It will include the following components:

- Planned Incident Process.
- Unplanned Incident Process.
- Incident Escalation.

A service change request is coordinated through the MSCI Service Desk. Either MSCI or State of Nebraska-designated personnel can initiate the requested service change. Service delivery and engineering staff will assess and identify the potential impact, risk, timeline, and costs associated with the functional change, hardware or component additions, and any required integration with additional systems or networks.

All service change requests follow the Change Management process, which includes the following steps:

- Create a service change request.
- Review and assess the change request.
- Develop an implementation plan for the change.
- Test the change.
- Determine a roll-back plan.
- Approve change.
- Review change performance.
- Close the change process.

1.6. Risk Management Plan

Our Risk Management process helps to ensure that the project team is making informed decisions about our approaches to identified risks and escalating high-profile risks to project stakeholders, both internally and externally, to manage the overall risk profile of the project and our respective organizations.

The risk analysis and management process includes four key activities:

- **Identification and Assessment:** Risk identification starts before a project is initiated, with the number of risks increasing as the project continues. The initial Risk Assessment attempts to identify, characterize, prioritize, and document a mitigation approach for risks identified at the start of the project. If the identified risk is determined valid through project assessment, the risk is assigned an owner and entered into the Risk Register as a Risk Statement.
- **Analysis:** Identified risks are analyzed to determine the probability of occurrence and impact on the project, which are used as the basis for assigning risk priority.
- **Planning:** Because mitigation approaches must be agreed upon by project leadership (based on the assessed impact of the risk, the project's ability to accept the risk, and the feasibility of mitigating the risk), time will be allocated in each project status meeting to identify new risks and discuss mitigation strategies. The Project Manager will convey amendments and recommended contingencies during the status meetings, or more frequently, as conditions may warrant. The most likely and highest impact risks are added to the project schedule to ensure that the project team takes the necessary steps to implement the mitigation response appropriately during the schedule.
- **Tracking and Control:** The Risk Assessment will be continuously monitored and updated throughout the project's life, with monthly assessments included in the status report and open to

amendment by the Project Manager. Assigned owners will manage ongoing risks and issues, with oversight by the Project Manager, and provide status updates on their assigned risks in the project team meetings. This task also includes a review of any residual risks.

During the project finalization process, the Project Manager will analyze each risk identified throughout the project and the Risk Management process's performance. Based on this analysis, the Project Manager will identify any improvements that can be made to the Risk Management process for future projects. These improvements will be captured as part of the lessons learned knowledge base.

Below is an example of the Action Items Register, Issues Log, and the Risk Register. The [Project Dashboard](#) will contain the register used during the project.

PRIORITY ACTION ITEMS							
ID	Description	Status	Priority	Date Raised	Date Needed	Assigned To (Full Name)	Notes
1							
2							
3							
4							
5							

ISSUES TO BE ESCALATED						
ID	Description/Impact	Priority	Date Raised	Assigned To (Full Name)	Impact if Not Resolved and Resolution Date or Mitigating/Contingency Actions	Comments
1						
2						
3						
4						
5						

RISK REGISTER									
ID	Risk Category	Risk Identified Date	Risk Identified By	Risk Description	Risk Action Plan	Action Owner	Current Status	Action Due Date	Status Update
1									
2									
3									
4									
5									

1.7. Project Punch List

The Project Manager will be responsible for creating, distributing, and maintaining a project punch list throughout the project life cycle until Final Acceptance. The punch list will be maintained in "real" time and is available within the Project Dashboard for key project participants.

Each punch list item will be assigned a severity level during acceptance testing, and any corrective action will be documented. If the punch list item cannot be corrected during the testing, it will remain open until the issue has been resolved to the satisfaction of both parties. Upon resolving a punch list issue, State of Nebraska's and MSCI's Project Managers will sign and date the punch list report to close it formally. Minor corrective action should not impact any previous test results.

The following is an example of the Project Punch List. The [Project Dashboard](#) will contain the punch list used during the project.

PROJECT PUNCH LIST								
ID	Priority	Description	Submitted By	Date Open	Owner	Target Completion Date	Current Status	Notes
1								
2								
3								
4								
5								

1.8. Quality Management Overview

The Project Management Plan includes Quality Management processes to minimize defects to the greatest extent possible and provide products and services that consistently meet specified requirements for performance, reliability, interoperability, usability, and documentation. We are committed to quality assurance, performing pre-release end-to-end system tests on our products with simulated traffic in our labs.

The Project Manager is the primary resource responsible for quality management, with other project team members supporting quality management. Team members may challenge existing processes to improve efficiency, eliminate unnecessary practices, or define and remediate process gaps.

MSCI follows ISO 9001 standards for quality to ensure the NG9-1-1 service meets the high standards required for public safety, such as:

- Providing controlled conditions for production, installation, and servicing. This control includes documented procedures, suitable equipment, and environment, compliance with documentation, process monitoring and control, approved equipment and processes, workmanship criteria, and preventative maintenance.
- Demonstrating the ability to consistently provide a solution that meets customer requirements and applicable statutory and regulatory requirements.
- Enhancing customer satisfaction through the effective application of quality standards, including processes for continual improvement and the assurance of conformity to customer and applicable statutory and regulatory requirements.

While MSCI uses a mature, defined, and audited quality management process to ensure that standards are met consistently, we continuously evaluate the impact to improve our process over time.

1.8.1. Quality Assurance and Control

MSCI performs quality assurance and control activities, including:

Documentation Control: Key project documents will be controlled through a centralized file repository. These documents will have versioning control fields. Document control entails appropriately naming and versioning project documents, templates, computer files, and other artifacts to ensure accuracy and relevance.

Testing: By testing the deployed solution in a controlled environment and executing functionality tests, MSCI and our customers have been able to capitalize on the benefits of improved system satisfaction.

Quality Reviews: Quality reviews are scheduled to review the findings from periodic audits. They are often conducted in conjunction with formal project meetings, whose audiences typically include MSCI's senior management members.

Quality Assurance: Business processes, policies, templates, and guidelines, provides the foundation for ensuring adherence to fundamental quality principles. Part of that is the Sales to Service (S2S) milestones and Certificates of Acceptance that are required in each project. These six (6) milestones are the gates of project delivery to ensure that the delivery equals the sale and meets contract and customer expectations every step of the way.

- S2S – Contract Signing
- S2S – Project Kickoff
- S2S – Customer Design Review Complete
- S2S – Go Live
- S2S – Handover to Support
- S2S – Final System Acceptance

Vendor Product and Service Quality: Our Global Supplier organization is responsible for identifying, vetting, and approving third-party providers of products and services. This organization reviews supplier business plans, processes, and performance annually or semi-annually, as needed.

Incident Reporting: Issues identified through quality management activities will be logged and reported to ensure that the issues are tracked and resolved throughout the project's lifecycle.

Monitoring and Measuring: Monitoring and measuring will focus on quality objectives and specific project requirements, including quality metrics unique to the State of Nebraska. We continually collect appropriate data to evaluate the suitability and effectiveness of the quality plan and implementation to determine if improvements can be made.

1.8.2. Quality Management Process

Throughout the project, the Project Manager will regularly take the following steps to monitor and ensure quality processes and standards are being followed.

- Manage and track the progress of team members and subcontractors:
 - Check and track milestone and/or deliverables adherence (customer-specific and S2S)
 - Check and track compliance to Key Performance Indicators, and perform the following tasks:
 - Track approved change requests.
 - Compare planned task completion with actual task completion.
- Identify potential risks or issues that may cause delays and ensure that mitigation plans are identified.

- Monitor risk items and determine the status of action plans, if any.
- Monitor end-user training plans.

The results of these tasks will be reported to the project team for continuous evaluation and improvement.

1.9. Governance Approach

Governance is critical for the end-to-end management of State of Nebraska's NG9-1-1 environment. The local MSCI teams have already established a reputation as a trusted source of industry expertise and advice with the State of Nebraska's governance body. MSCI will continue to build on that rapport to advocate for the State of Nebraska and PSAP interests. We are also committed to assisting and communicating with any other governing body if the State of Nebraska requires it.

Throughout implementation, MSCI will work closely with the State of Nebraska to design a successful implementation strategy with input from the State of Nebraska to ensure that the needs of the local PSAPs are being addressed.

Operationally, MSCI will serve in an advisory role, reporting key metrics on the operational health of the service. MSCI is prepared to report to the State of Nebraska's committees and governance body at key meetings when needed. MSCI will report maintenance metrics for the NG9-1-1 service to the State of Nebraska and suggest ways to enhance the capabilities of the deployed Service further.

MSCI understands that successfully implementing the new NG9-1-1 Service is critical to the State of Nebraska, the governance body, and most importantly, citizens and first responders. As a true end-to-end public safety communications company, MSCI is committed to working with the State of Nebraska and all governing agencies to ensure that implementation, operation, and maintenance are performed to the mission-critical level of service required.

Section 2

Project Implementation Plan

The following sections describe the scope of work associated with the major tasks performed when implementing the new NG9-1-1 system. Each major task is described along with a Work Breakdown Structure, which defines the responsibilities of MSCI and State of Nebraska.

2.1.1. Detailed Design Review

Following the kick-off meeting, the Detailed Design Review process will begin, during which the project's functional, deployment, and service aspects are reviewed and confirmed. The preliminary design and implementation plan provided will serve as a baseline for the Detailed Design Review. Any changes determined in the Detailed Design Review will be documented through a Change Order.

MSCI will meet with the participating Customer stakeholders and perform a review of the proposed NGCS/ESInet/NG9-1-1 services. During this meeting(s), information specific to the operational environment of the Customer and the PSAPs will be gathered to understand how best to approach the migration to the NGCS/ESInet solution. The data gathered will include, but is not limited to, the following:

- Confirmation of bandwidth figures and requirements.
- Information on PSAP operations and PSAP jurisdiction boundaries.
- Each region or PSAP's plans and timing for migration to NG9-1-1 and/or timing to make that decision.
- Initial sequencing and grouping of regions or PSAPs with respect to joining the NGCS/ESInet.
- Information regarding all other relevant PSAP projects or programs (NG9-1-1 call handling, logging, recording, LMR, CAD, etc.) to plan for constraints and dependencies.

Tasks	MSCI	State of Nebraska
Review functional requirements, locations where equipment will be installed and site responsibilities, circuit requirements, and responsibilities, and update the Solution Description as needed.	X	X
Identify external 3rd party product interface requirements.		X
Review demarcation between MSCI-supplied equipment and the Customer interfaces.	X	X

Review the Work Breakdown Structure, which includes Project Tasks and Responsibilities. Review and update the Project Schedule as required.	X	X
As necessary, update Design Documentation, which may include an updated Solution Description, Project Schedule, Acceptance Test Plan, Preliminary Migration Plan, Training Plan, Documentation, Customer Support, and Emergency Preparedness.	X	
Provide Milestone Acceptance Certificate for Signature	X	
Sign Milestone Acceptance Certificate	X	X
Execute Change Order via the agreed upon Change Management plan in accordance with all material changes to the Contract resulting from the Design Review.	X	X
The solution is "frozen" in preparation for subsequent implementation tasks such as equipment and services, order processing, and manufacturing.	X	X

2.1.2. NGCS Installation and Provisioning

The conclusion of the detailed design review begins the start of service provisioning.

Tasks may include the expansion of core routing services and networking appliances, including (not limited to):

Core Routing Functions

- Border Control Function (BCF)
- Emergency Services Routing Proxy (ESRP)
- Emergency Call Routing Function (ECRF)
- Location Validation Function (LVF)
- Location Database (LDB)
- Management and Services Dashboards
- Domain Name Service (DNS)
- Network Switches and Routers
- Spatial Interface (SI)
- Location Database Management System

The core routing service provisioning work breakdown structure is in the table below.

Tasks	MSCI	State of Nebraska
Create equipment orders and reconcile to the contract in accordance with final approved Detailed Design Review documents	X	
Configure Next Generation Core Routing services: • Border Control Function • Emergency Services Routing Proxy • Policy Routing Function • Spatial Interface • Emergency Call Routing Function • Location Validation Function • i3 Event Logging	X	
Participate in the review and creation of policy routing functions		X
Provide GIS data that will be used within the ECRF & LVF subsystems		X
Provision Legacy Selective Router Gateways (LSRG) as required	X	
Provision Legacy Network Gateways (LNGs) as required	X	
Provision and test inter-NGCS peer IP connections	X	
Provision firewalls, routers, and Session Border Controllers (SBC)	X	
Provision NGCS POPs and Functional Elements for the Service	X	
Provision i3 event logger and associated network connectivity	X	
Assess customer provided GIS vs. requirements and provide written summary to customer	X	
Submit required GIS data layers to the Spatial Interface		X
Provision Location Database	X	
Provision ECRF and LVF via the Spatial Interface (SI)	X	
Provision and test ESInet network, to validate compliance with MSCI established networking and bandwidth documentation	X	
Provision relevant remote access facilities	X	

2.1.3. Ingress Network Implementation and Carrier Migration

After receiving Letters of Agency (LOA) from the State of Nebraska, MSCI will begin the carrier migration process by distributing notifications to the carriers. Network change notifications, specifically tailored for each carrier, will provide at least four months of lead time for the carriers to implement new trunking arrangements. Carrier migration is a critical path item.

Circuit Path Order, Delivery, Technology

MSCI's team of specialists will work with the numerous carriers and service providers supporting the State of Nebraska to coordinate the delivery of circuit paths to the MSCI-designated Points of Interconnect (POIs) and Meet Points. The team also ensures the carrier circuit paths adhere to redundancy and diversity requirements.

Based on the due dates provided by MSCI's team, carriers will submit facility orders to Meet Points or POIs to access the Legacy Network Gateways for the MSCI NGCS Service. Carriers also have the ability to deliver 9-1-1 services via Session Initiation Protocol (SIP), in which case carriers will be required to deliver dedicated IP circuits to the MSCI POIs. Carriers are instructed to order diverse trunk groups to the MSCI NGCS Service.

Legacy Selective Router Gateways (LSRGs)

The NGCS routing service can support LSRGs to enable calls to be routed and/or transferred between legacy PSAPs served by legacy selective routers.

Traffic Migration Process

MSCI will manage the traffic migration process to ensure continued traffic delivery to the PSAP during the migration. The legacy selective router and the NGCS routing service direct call traffic cooperatively until traffic is migrated. The migration process is conducted so that it is possible to back out and revert to the original routing mechanism should an issue be discovered during migration. This ensures calls will continue to be delivered to the PSAP during implementation.

The ingress implementation steps include:

- The carrier establishes connectivity to the MSCI Point of Interconnect (POI).
- Test circuits at the POIs.
- Generate test calls from the carrier(s) to the NGCS routing service to the NG9-1-1 call handling solution.
- Perform carrier migration:
 - Migrate individual VoIP service provider traffic (e.g., Vonage) from legacy selective router to MSCI NGCS Service.
 - Test and confirm VoIP calls are successfully migrated.
 - Repeat for all VoIP service providers.

- Migrate individual Wireless service provider traffic (e.g., T-Mobile) from legacy selective router to MSCI NGCS Service.
- Test and confirm wireless calls are successfully migrated.
- Repeat for all wireless service providers.
- Migrate individual Wireline service provider traffic (e.g., AT&T) from legacy selective router to MSCI NGCS Service.
- Test and confirm wireline calls are successfully migrated.
- Repeat for all wireline service providers.
- Migrate each carrier's call traffic from the legacy router to NGCS routing service.
- State of Nebraska submits an order to the Local Exchange Carrier to remove analog 9-1-1 trunking from the legacy 9-1-1 system.
- Manage the transition from implementation to Service Operations and ensure that the documents for MSCI NSOC are accurate to identify, triage, and remedy any issues that arise with carriers during normal operations.

The ingress network implementation and carrier migration work breakdown structure are in the table below:

Tasks	MSCI	State of Nebraska
Prepare carrier migration to the MSCI NGCS Service based on agreements, plans, and timeline established with each carrier	X	
Transition to Service Operations and Support	X	
Deem Service ready for Acceptance Testing	X	
Execute carrier migration according to the call taker migration plan	X	
Execute orders to carriers to remove legacy 9-1-1 trunking services once the carrier migration and call taker migration process is complete		X

2.1.4. Egress Network Implementation (ESInet)

In parallel with ingress network implementation, the project team will implement the PSAP egress connections. This ensures the ESInet network termination equipment configuration is planned and completed following the project schedule.

The egress network design steps include:

- Identify all involved public safety 9-1-1 call delivery locations or endpoints.
- Validate bandwidth requirements.
- Assess redundancy and diversity capability for region or PSAP egress connectivity.

- Procure egress network segments per diversity and bandwidth requirements.

The egress network implementation work breakdown structure is in the table below:

Tasks	MSCI	State of Nebraska
Provision ESInet network connections to each Call Handling System (CHS) Host Site/PSAP	X	
Exercise ESInet circuit redundancy / diversity	X	
Provide diverse circuit entry facilities at each PSAP		X
Perform network turn-up for testing	X	
Perform Quality of Service and bandwidth verification testing on ESInet network segments	X	
Confirm connectivity between the call handling and core routing subsystems	X	
Confirm the ESInet is ready to support PSAP migration	X	

2.1.5. Location Database (LDB) Data Migration

The replacement of the existing legacy Automatic Location Information (ALI) service with an NG9-1-1 compliant Location Database (LDB) will occur in two or three phases depending on how the State of Nebraska intends to deploy and manage their location related data.

Phase 1

In the first phase, the incumbent ALI provider will provide MSCI with a snapshot of the current ALI database or MSAG and ALI files if no current ALI database exists to build the MSCI LDB. This data is assessed and the cleanup of legacy data is initiated. This partnership will be between MSCI, the State of Nebraska, and local addressing authorities to ensure the LDB holds valid data for use in NG9-1-1. Records will be flagged as representing true civic addresses vs. wireless/VoIP shell records, Foreign Exchanges, or test TNs. Wireless shell records will be populated with X/Y coordinates representing their PSAP route for when a device location is unavailable during the call.

Phase 2

This phase typically starts just prior to Location Services go-live activities. However, this phase will start sooner to accommodate testing activities. During this phase, MSCI will manage the dual provisioning process of SOI files which will occur until all OSPs have been migrated. Each record in these SOI files is validated against the MSAG and rejected (sent back to the OSP) if no match is found. If MSAG Conversion Service and/or CLDXF (Civic Location Data Exchange Format) is part of the project, valid SOI

records are then compared to the GIS data within MSCI MSAG Conversion Service, and if CLDXF complementary values are found, a CLDXF record is also generated in the LDB. This allows the LDB to respond both to ALI requests with traditional ALI and to HELD requests with PIDF-LO using the CLDXF.

Phase 3 (If Applicable)

When the Phase 2 migration is complete, Motorola will work with the State of Nebraska to generate a GIS-derived MSAG. This GIS-derived MSAG will replace the civic addressing records within the current MSAG once no ALI records are left invalid (orphaned). When all ALI records validate, the new MSAG will be maintained on a scheduled basis from the Spatial Tools provided. As new GIS-derived MSAGs are generated, they are compared to the existing MSAG, changes are updated, and the ALI is revalidated before placing it in use. Any discrepancies during the process are sent back to the State of Nebraska for remediation. Once a GIS-derived MSAG is placed in use the SOI records will technically be validating against the GIS data, thereby ensuring a match to the ECRF data during the 9-1-1 call flow.

MSCI will work closely with the State of Nebraska during LDB data migration to the new NGCS Location Service to ensure that the most current data is replicated, that the data contains no standards-based issues, and ensure data update processes are in place.

Tasks	MSCI	State of Nebraska
Coordinate with State of Nebraska to obtain the most recent MSAG and ALI report	X	
Gather and provide the most recent MSAG and ALI report		X
Perform Data Validation and check for errors	X	
Provide State of Nebraska with a report and discuss any standards-based issues that should be resolved	X	
View service provider discrepancies to identify any pending issues	X	
Load import data into the NGCS Location Service and test data accuracy	X	
Perform import of the most current dataset prior to service migration	X	
Establish and coordinate a data maintenance process with the service providers	X	
Allow service providers, including Multi-Line Telephone System (MLTS) operators, to submit Service Order Input (SOI) records (Moves, Add, Change, Delete) and customer MSAG changes via the customer Database Management System (DBMS web portal) and/or an sFTP automated service	X	

Tasks	MSCI	State of Nebraska
Scan for viruses and save records received into the DBMS and/or SFTP server	X	
Update the redundant Location Databases	X	
Implement automatic data updates to MSCI NGCS	X	

The LDB migration work breakdown structure is in the table below:

2.1.6. NGCS Data Provisioning

MSCI will provision PSAP configurations in the MSCI NGCS Service using the information gathered during policy route plan (aka callflow strategy) planning meetings. This data collection includes current and desired operational policy routing rules that each served PSAP utilize today and/or require in the immediate future.

Working closely with the State of Nebraska, the MSCI project team will design a policy route plan that best supports customer operational workflows. Location services provisioning is part of the migration process and will include data required from the State of Nebraska to enable call routing and transfer scenarios.

The NGCS data provisioning work breakdown structure is in the table below:

Tasks	MSCI	State of Nebraska
Collection of existing and planned call routing and transfer flows	X	
Design the provisioning plan	X	
Participate in the provisioning plan and provide guidance relative to State of Nebraska operational workflows		X
Assist validating the plan throughout the acceptance test and migration process		X
Provision mutually agreed upon callflow plan	X	

Section 3

PSAP Transition/Migration Plan

The transition plan provides the transition from the legacy call routing system to the Next Generation Core Services (NGCS) solution while ensuring the integrity of State of Nebraska's existing, mission-critical 9-1-1 services.

The plan's foundation relies on constructing the new Next Generation Core Routing Service and ESInet alongside the legacy call routing solution. The transition process involves the migration of call delivery from individual wireline, wireless, and VoIP carriers to the ingress of the new NGCS and delivering calls to individual PSAPs via the new ESInet egress service.

This plan is preliminary in nature and illustrates the fundamental process and diligence MSCI will demonstrate. The final transition plan will account for the attributes and constraints posed by individual PSAPs (e.g., call volume, standard operating procedures, and workflows).

The transition plan addresses the following major elements:

- System Construction.
- Carrier Identification and Call Volume Analysis.
- OSP Ingress Design.
- Reliance on Legacy Selective Routers and ALI Database Services.
- Validation of Ingress from Carriers to the new Core Routing Service.
- ESInet Egress Design.
- Validation of Continuity among Carriers, MSCI, and PSAPs.
- Methods of Testing.
- Potential Disruptions to Existing and New Operations.

In addition, throughout the implementation of the new system, leading up to the PSAP migration process, MSCI and State of Nebraska will conduct detailed migration planning sessions to identify:

- Standard operational procedures.
- Risk identification and mitigation.
- State of Nebraska responsibilities (e.g. readiness of call handling systems, required staffing resources, optional resources).

MSCI offers the enclosed transition plan as a basis from which MSCI and State of Nebraska can fine-tune the plan through a process that results in a better understanding of State of Nebraska's operational requirements and tailoring the plan to suit the desired outcomes for both State of Nebraska and the PSAPs.

3.1. System Construction

Next Generation Core Services (NGCS) functional elements will be located at multiple locations across the United States, that comprise MSCI's overall NGCS infrastructure. The core routing solution will interface with each hosted or standalone 9-1-1 call handling system throughout the State of Nebraska.

The transition plan starts with the construction of the new routing service and ESInet. The new system will be constructed alongside the existing system such that the new system will be operational and fully tested before moving "live" call-routing operations to the new system.

3.1.1. NGCS Elements

MSCI's NGCS infrastructure includes redundant and geographically diverse NGCS elements. The NGCS network architecture provides:

- Geographic diversity and redundancy of all NGCS Elements.
- Point of Interconnection (POI) and Border Control Function for Carrier 9-1-1 Call Traffic Inbound to the NGCS Routing service.
- Border Control Function for Delivery of 9-1-1 Call Traffic to the State of Nebraska's PSAP(s).
- Legacy Network Gateways, Legacy Selective Router Gateways, and Points of Interconnect for delivering IP-based and TDM-based 9-1-1 call traffic into the carrier migration network.

These efforts will result in the interconnection of OSPs to MSCI's network without infringing upon State of Nebraska's existing legacy 9-1-1 infrastructure. The result will include an environment where tests can be conducted with individual carriers by generating test calls that flow from a carrier, through the carrier migration network, into the NGCS routing platform.

3.1.2. ESInet Connectivity

The ESInet solution will provide connectivity for the egress of calls from the NGCS routing platform to State of Nebraska's Call Handling Systems and/or PSAPs. ESInet circuit orders, construction, and installation will result in connectivity that does not rely upon or interfere with any of State of Nebraska's existing wide-area network connections. With this approach, a completely new set of wide area network connections will be installed and tested in a manner that is transparent and non-intrusive to State of Nebraska's (and individual PSAPs') existing 9-1-1 operations.

3.1.3. PSAPs and Call Handling Host Elements

MSCI's ESInet will provide the egress of calls from the NGCS solution to individual PSAPs. At each PSAP, the ESInet will terminate on MSCI-supplied network equipment – specifically, the LAN-facing port of the MSCI ESInet (Edge) router.

State of Nebraska is responsible for providing call handling systems that comply with the [MSCI NGCS Service PSAP Interface Specification / User to Network Interface \(UNI\) requirements](#) for interconnection to the MSCI NGCS service to include NENA i3-bashed calls, SMS-based text to 9-1-1, Real Time Text, etc. Professional services supporting firewall configurations (routing and Text to 9-1-1) and call handling system architecture or field engineering work associated with any call handling system upgrades are the responsibility of the State of Nebraska.

The PSAPs that are part of the NGCS and ESInet implementation are listed in the table below, along with MSCI's understanding of which call handling system that each PSAP is operating currently. Release versions will be determined during PSAP data gathering.

PSAP Name	City	County	CHS

The PSAPs listed below are designated as "Optional" and are not part of the NGCS and ESInet implementation. However, they represent possible transfer destinations for several of the PSAPs referenced above.

PSAP Name	City	County	CHS

PSAP specific information for all referenced PSAPs including but not limited to address, point of contact information, vendor information (call handling system specifics, CAD, logging recorder), legacy routing information, and telecom facility information is maintained in the [Project Dashboard](#) for easy reference.

3.2. Carrier Migration, Ingress, and Egress Network Validation

3.2.1. Carrier Identification and Call Capacity Analyses

MSCI identifies the technology currently utilized by each carrier in the transport of 9-1-1 call traffic. The type of signaling or technology currently used by each carrier will have an impact on the carrier migration networking design.

MSCI will extend to each OSP the following methods of call handoff to the MSCI NGCS network, listed in order of preference: NENA i3 Session Initiation Protocol (SIP), Basic SIP, or Signaling System 7 (SS7). MSCI will prioritize the use of IP-based transport mechanisms as the preferred method for OSPs to deliver traffic to the migration backbone, though ultimately, the decision is made by the respective OSP.

3.2.2. Ingress to the Call Routing Service

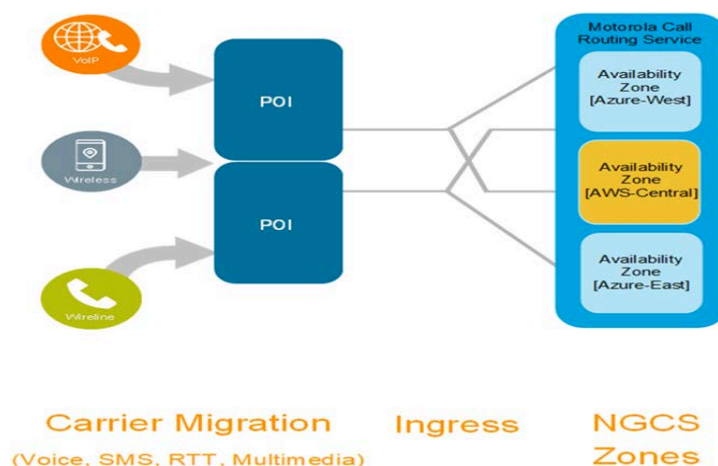
MSCI has an established carrier migration methodology that will be applied to the ingress of calls to the NGCS routing platform. This effort will include finalizing the methods that carriers and/or the incumbent call routing service provider will continue or adopt to continue the delivery of calls to the existing PSAPs up until the time individual carriers are cut over to the new system. MSCI coordinates with PSAPs, carriers, and the incumbent 9-1-1 call routing service provider(s) to successfully transition calls to the new NGCS solution.

3.2.3. Migration and Validation

The process of carrier migration and validation of successful call delivery includes:

- Identifying all wirelines, wireless, and VoIP carriers and analyzing their individual maximum simultaneous call capacities.
- Determining the method of call handoff that each OSP will use to deliver calls to the MSCI call routing network.
- Determining the process by which 9-1-1 call traffic will continue flowing to the individual PSAPs up until the time of individual carrier migration and migration to NGCS. This includes interconnection between MSCI and the incumbent call routing service provider. This enables the carrier migration process to occur in parallel with PSAP migration in a controlled, methodical process.
- Validating the ability to send 9-1-1 test calls from each OSP, through the migration network, through the MSCI NGCS call routing network, and to the PSAP.

Carrier Migration – Ingress Design



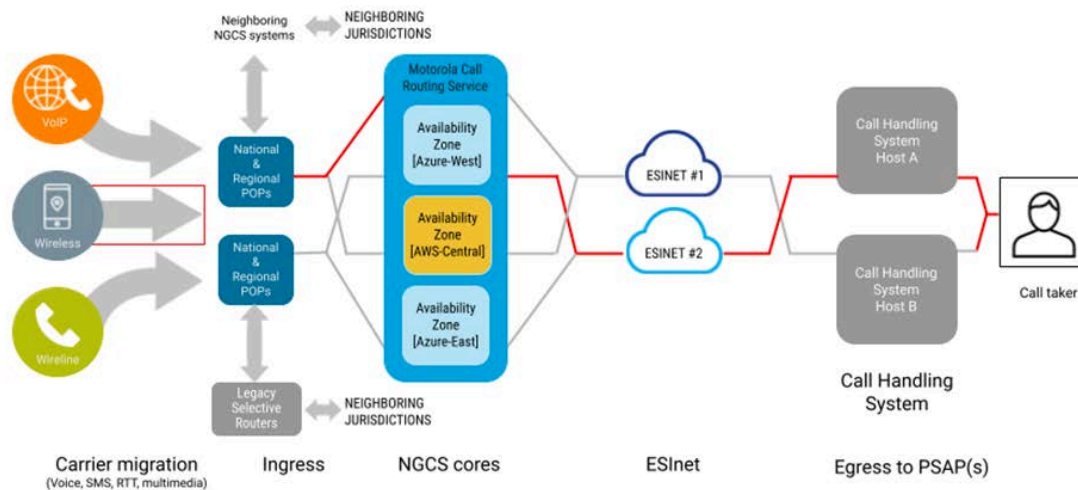
In the migration state illustrated above, individual OSP connections to MSCI network are tested to confirm that test 9-1-1 calls from each OSP flow through the MSCI call routing service network. MSCI will work with individual OSPs to define the process and required networking topology, routes, etc.

Testing individual OSP call-flows through the MSCI network validates continuity between the OSPs and the MSCI NGCS network. This process will validate individual OSP readiness to migrate 9-1-1 call traffic from the existing 9-1-1 call routing service provider to the MSCI NGCS network. By accounting for individual carrier call volumes, and the pace/quantity at which individual PSAPs will migrate to the MSCI NGCS service, MSCI will work with the State of Nebraska and the PSAPs to create a migration plan that establishes the time and date at which carriers will migrate their traffic to MSCI. The plan will also include a fallback mechanism for OSPs to divert calls back to incumbent systems should disruptions prohibit executing the migration plan.

3.2.4. ESInet Connectivity and NGCS Egress Network Validation

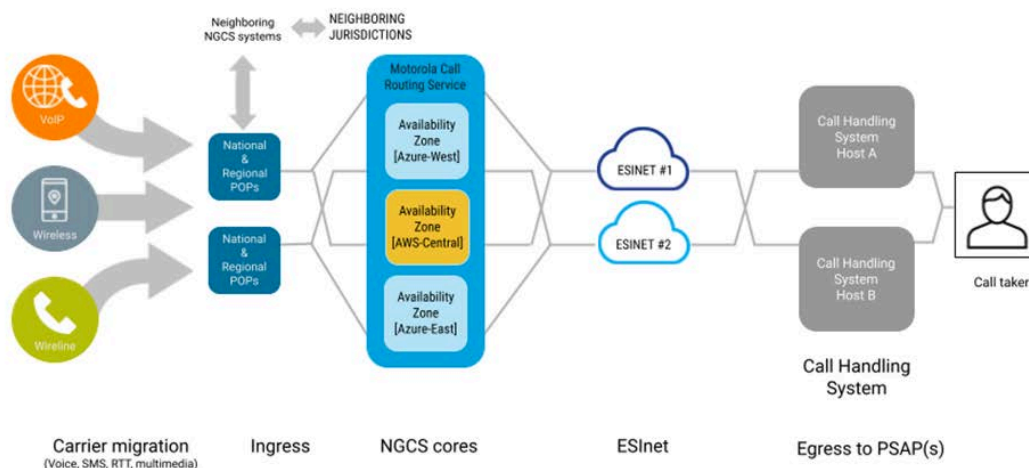
In addition to the ingress validation process described above, MSCI will validate call-flow connectivity through the NGCS call routing service to the above-mentioned LAN-facing port of ESInet edge termination routers at each PSAP call handling system. Test calls will flow through the newly constructed network without affecting State of Nebraska ongoing operations. The drawing below illustrates the flow of test calls from individual OSPs.

Call in Progress - Any OSP to PSAP via Any Path



By validating call-flows from individual OSPs to the PSAPs, MSCI can confirm the planned project end-state of the architecture that will exist at the completion of the OSP migration and migration process. The diagram below represents the planned project end-state, after which each OSP sends 9-1-1 calls through the MSCI NGCS / ESInet solution.

NG9-1-1 End State without Legacy elements



Not for use or disclosure outside Motorola Solutions Connectivity, Inc. without written permission.

The MSCI NGCS call routing service only ingresses 9-1-1 calls from OSPs (carriers). Once a 9-1-1 call is received, the new NGCS call routing service routes the call to the appropriate PSAP.

3.3. Migration Planning

By simulating test calls from individual OSPs and by constructing the new NGCS solution alongside the existing network, all of the aforementioned validation processes will occur without infringing upon State of Nebraska existing 9-1-1 operations. Once these validations are complete, the process of finalizing the migration plan can begin. Finalizing the plan will ensure the unique needs of the PSAPs are addressed while ensuring successful call routing.

3.3.1. Acceptance Testing

Prior to executing the migration plan, MSCI will execute System Acceptance Test plans, which will verify the successful operation of the NGCS solution. Types of testing includes:

- Ingress of Calls from Originating Service Providers.
- Routing of Calls to Individual PSAPs.
- Routing Policy Verification.
- NGCS Failover Testing.
- Network Failure and Recovery.
- Call Processing during Call Handling System Host and Network Failure and Recovery.

3.3.2. Migration Plan

The migration plan builds upon the foundational elements established in the preceding sections, which are summarized here:

- Complete construction of the new service (NGCS and ESInet) alongside the existing system.
- Carrier call-capacity analysis to provide input to the migration plan.
- Methodical migration of carriers and testing to validate call-flows from OSPs to PSAPs.
- Detailed functional system acceptance testing, which exercises all NGCS call routing service aspects.

The following sections illustrate the steps that will be taken to migrate the OSPs and PSAPs to the new routing solution.

3.3.3. OSP and PSAP Migration to the New Routing Service

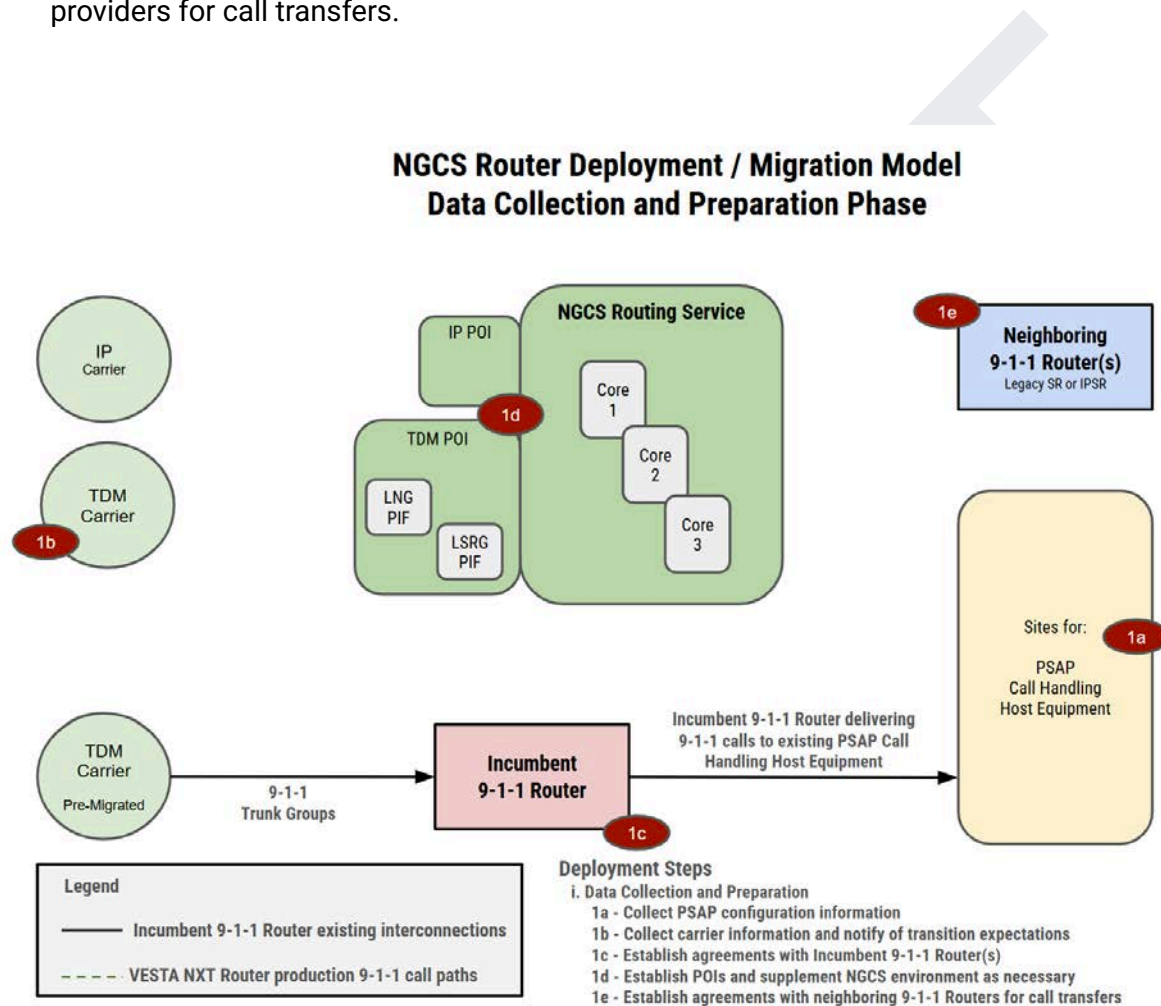
The following sequence of activities and illustrations provide a preliminary model for the deployment of the NGCS call routing service and the migration of carriers. This model will be used as a baseline for a detailed design review and adjusted through collaboration with the State of Nebraska.

- Provision required elements for the deployment of NGCS call routing and ESInet infrastructure.
- Identify, notify, and start migration planning of the OSP serving the State of Nebraska PSAPs.

DRAFT

Data Collection and Preparation Phase:

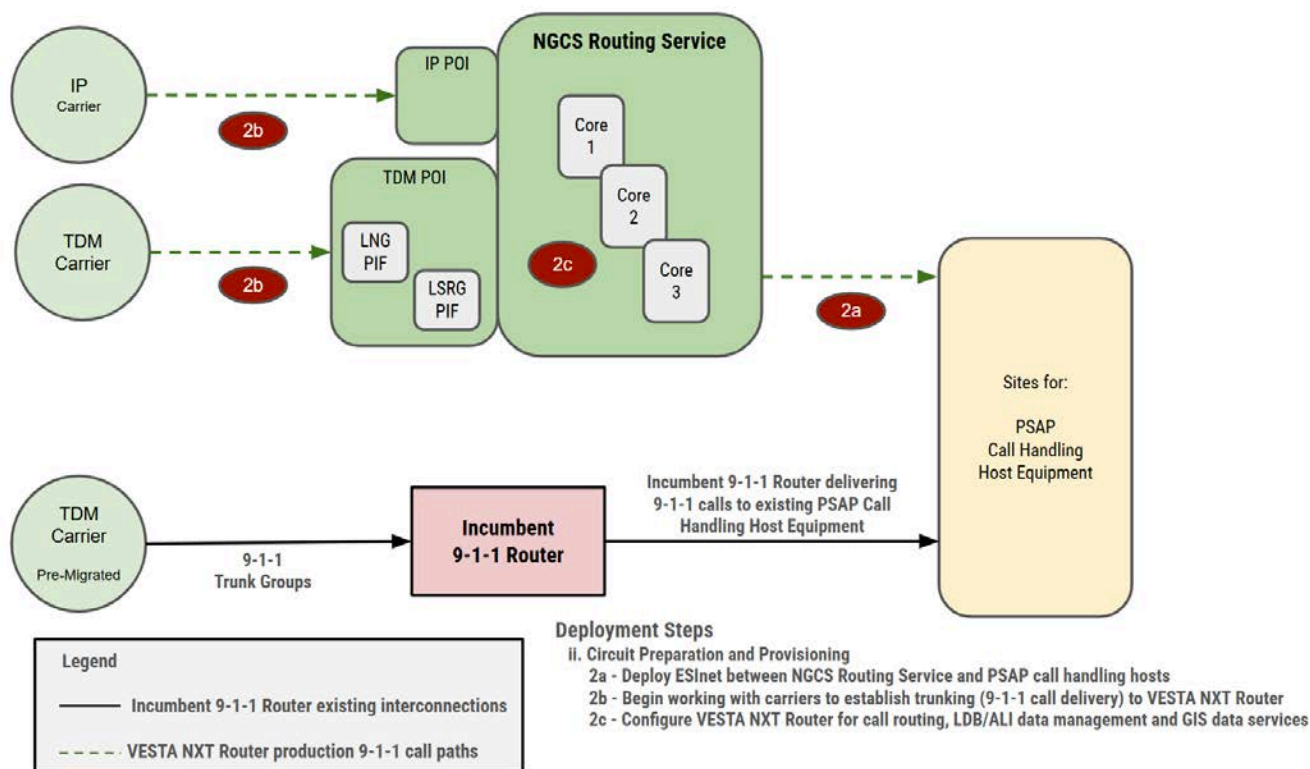
- Collect PSAP configuration information.
- Collect OSP information and notify each of the transition expectations.
- Establish TDM Points of Interconnect (POIs) within the State of Nebraska's LATAs.
- Leverage existing interconnection agreements with neighboring 9-1-1 call routing service providers for call transfers.



ESInet Preparation and Provisioning Phase:

- Deploy ESInet between NGCS and PSAP call-handling hosts.
- Work with OSP to establish interconnection to the NGCS routing service.
- Configure the NGCS routing service for call routing, LDB, and location data management services.
- Establish connectivity to neighboring 9-1-1 call routing service providers), as required (not illustrated).

NGCS Router Deployment / Migration Model Circuit Preparation and Provisioning Phase

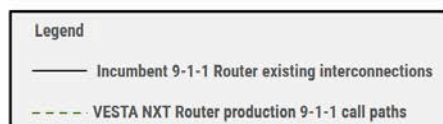
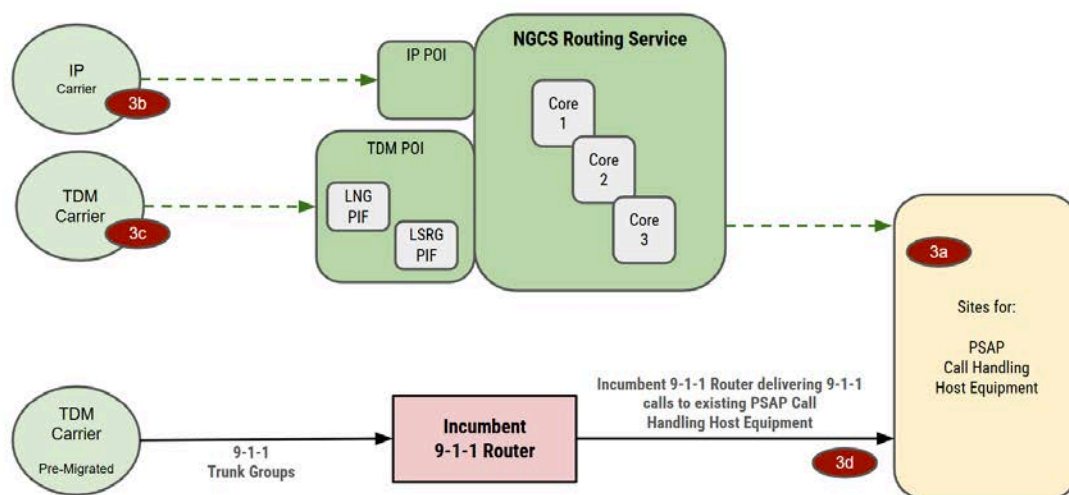


Not for use or disclosure outside Motorola Solutions Connectivity, Inc. without written permission.

Migration Phase:

- Migrate PSAPs to NG9-1-1 call routing by working with OSP to deliver 9-1-1 calls to the NGCS routing service,
 - Coordination with State of Nebraska PSAPs, OSP, and incumbent 9-1-1 call routing service provider(s),
 - OSPs direct their SIP based 9-1-1 traffic to the NGCS routing service via SIP POIs designated by MSCl.
 - OSPs direct their TDM based 9-1-1 traffic to the NGCS routing service via TDM POIs designated by MSCl.

NGCS Router Deployment / Migration Model Migration Phase



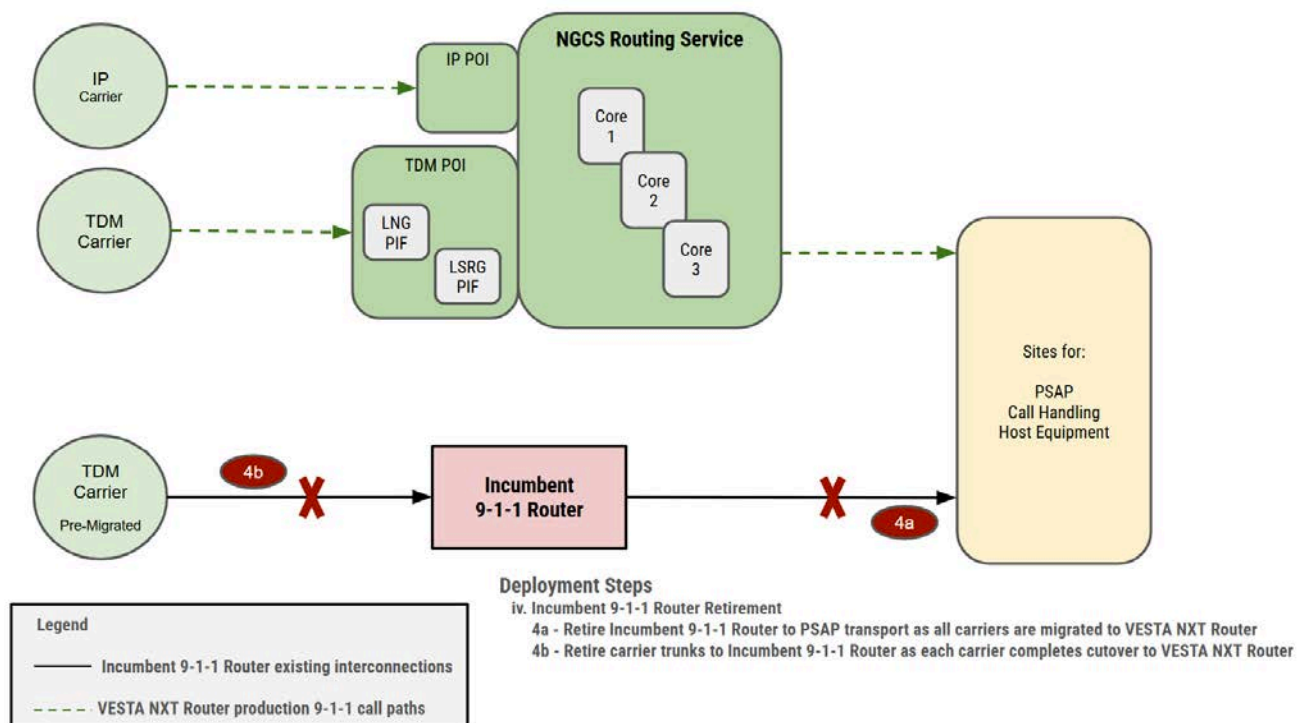
Deployment Steps

- iii. Migrate PSAPs by transitioning 9-1-1 calls to VESTA NXT Router
 - 3a - Coordination with 9-1-1 Authority, PSAPs, Carriers, and Incumbent 9-1-1 Router
 - 3b - IP-based carriers direct 9-1-1 traffic to VESTA NXT Router via IP POI for delivery to NG9-1-1 call handling system
 - 3c - TDB-based carriers direct 9-1-1 traffic to VESTA NXT Router via TDM POI for delivery to NG9-1-1 call handling system
 - 3d - Once all carriers (one-by-one) are directed to VESTA NXT Router, 9-1-1 calls no longer delivered to incumbent 9-1-1 Router

Incumbent 9-1-1 Router Retirement Phase:

- Incumbent 9-1-1 call routing service provider retires PSAP transport between Incumbent 9-1-1 call routing service provider and PSAP call handling systems.
- OSPs retire OSP facilities to Incumbent 9-1-1 call routing service provider as each OSP completes its migration to the MSCI NGCS routing service.

NGCS Router Deployment / Migration Model Retirement Phase



3.3.4. Legacy Selective Routers and ALI Data

Legacy Selective Routers

As illustrated in the carrier migration process above, the end state of the migration negates the need for Legacy Selective routers (LSR). While the LSR is utilized during the migration, it is no longer needed once all carriers migrate to the new routing service.

ALI Data

As described in the project implementation plan, the Location Database (LDB) migration process includes the transition from the incumbent ALI provider such that all OSPs will cease sending their ALI updates to the incumbent ALI provider and begin sending updates directly to the MSCl location database management system.

3.4. PSAP Migration

Once MSCl constructs and tests the Ingress and Egress ESInet networks, a major activity will be for the State of Nebraska to migrate their PSAP positions onto the new NG9-1-1 network.

This step will require coordination between MSCl and State of Nebraska teams. The PSAP migration methodology will be agreed upon during the Detailed Design Review of the project initiation and planning phase.

MSCl will implement an ESInet edge termination router(s) to each call handling host location in parallel to any existing network hardware from the existing Incumbent call routing provider. The PSAP CHS will then enter into "Dual PSAP" mode, where the PSAP CHS will be able to handle 9-1-1 calls from both the ESInet and the Incumbent router. If "Dual PSAP" mode is not viable, alternative migration strategies will be implemented.

MSCl will then, one by one, migrate call traffic from each OSP to delivery via MSCl's network. Once all the OSPs have been migrated to the MSCl network and it is verified that all CHSs are functioning properly, incumbent 9-1-1 service provider call delivery facilities to the call handling systems/PSAPs may be retired by the respective incumbent 9-1-1 call routing service provider.

State of Nebraska will be responsible for providing MSCl access to PSAP facilities for the installation of ESInet edge termination equipment. State of Nebraska will also be responsible to engage the CHS providers in each PSAP to switch CHS equipment from Incumbent 9-1-1 call routing service provider to the MSCl network.

The final plan for the sequence of PSAPs as they transition to the MSCl network will be discussed and agreed upon during the Detailed Design stage.

3.5. Text to 9-1-1

Text to 9-1-1 is the ability to receive 9-1-1 requests for emergency assistance from mobile devices. There are two primary methods that citizens can utilize to communicate via text to the MSCI call routing service, which include Short Message Service (SMS) and Real Time Text (RTT).

Historically, SMS Text to 9-1-1 traffic was delivered from OSPs via an originating Text Control Center (TCC) to the intermediate TCC that was designated by the jurisdictional 9-1-1 authority, which in turn delivered the SMS text traffic via Message Session Relay Protocol (MSRP) over SIP to MSCI 9-1-1 call routing network for routing to the appropriate PSAP.

On July 19, 2024, the Federal Communications Commission (FCC) approved an NG9-1-1 Report and Order (R&O) that put in place new requirements for all OSPs in the United States to deliver all 9-1-1 requests for service (including voice, text, multimedia, etc.) from their subscribers via Session Initiation Protocol (SIP) to Points of Interconnection (POI) stipulated by the jurisdictional 9-1-1 authority. This negates the requirement for 9-1-1 authorities to contract for intermediate TCC services. In the wake of this order, OSPs will be required to deliver SMS text to 9-1-1 traffic directly to the POIs designated by the 9-1-1 Authorities, which MSCI will designate in coordination with the State of Nebraska.

RTT Text to 9-1-1 traffic is delivered from the OSPs via the same infrastructure as 9-1-1 voice calls that OSPs remit to MSCI's call routing network using the SIP protocol. RTT is simply an additional payload within the voice call session. RTT will be implemented for the State of Nebraska at a point in the future, following the initial MSCI call routing service deployment, following mutual agreement between State of Nebraska and MSCI.

3.6. Interoperability

The MSCI NGCS Service includes interoperability with peer regionally adjacent 9-1-1 networks. Transfers to and from the neighboring areas will be supported via 9-1-1 and/or PSTN technologies as mutually agreed upon between MSCI and the respective relevant peer 9-1-1 call routing providers.

3.7. Migration Phases

Migration to the new service consists of three phases: Pre-Migration tasks, the Migration event, and Post-Migration tasks.

3.7.1. Pre-Migration Tasks

The pre-migration task list is essentially a checklist that must be reviewed and verified completely to ensure the success of the migration. All system integration, acceptance testing, and training activities must be completed before any PSAP migration. Pre-migration activities will ensure that all migration and

fallback procedures are in place and that all systems perform as expected. Below are the typical tasks that will be performed by MSCI and PSAP stakeholders to prepare for migration.

Tasks	MSCI	State of Nebraska
The Customer is responsible for providing the facility space, commercial power, backup power, grounding, and cable entrance facilities necessary to accommodate the Router Edge equipment.		X
Develop and approve the Policy Route Plan (e.g., PSAP list, primary, alternate, busy, overflow, transfers).	X	X
Develop a draft Migration Plan and "Ready for migration" dates.	X	
Provide final approval of the Migration Plan		X
Distribute the Migration Plan and event invitations to all key individuals	X	X
Coordinate closely with the PSAP to mitigate disruptions of service during the migration	X	
Conduct pre-migration acceptance testing of MSCI and customer-provided subsystems to include wireless, wireline and Voice over IP provider 9-1-1 calls	X	
Ensure all PSAP personnel are made fully aware of the NG9-1-1 migration date and time, including: • Third-party vendors, as needed. • Neighboring, backup, and supporting PSAPs/dispatch agencies. • Other organizations/agencies that are participating in the migration or will be impacted to any degree during the migration.		X
Coordinate third-party services and/or activities during the migration that are not MSCI deliverables, but impact MSCI systems and/ or services.		X
Confirm no special activities are planned which could prevent or delay the migration.	X	X
Identify and implement Call Handling System changes to support the migration to NGCS (location services, voice, and Text to 9-1-1) while supporting a fallback plan		X
Complete all applicable training		X
Review and finalize the Customer Service and Support Plan as provided by MSCI.		X

3.7.2. Migration Tasks

The actual Migration is the process of bringing the new systems/services into beneficial use. The migration will consist of systematically transitioning 9-1-1 call routing to the NGCS platform.

Tasks	MSCI	State of Nebraska
Ensure Post-Migration support staff are notified and ready.	X	X
Notify all impacted internal departments, external agencies, and institutions of the Migration Plan.		X
Execute the migration plan for NGCS and ESInet	X	
Execute the migration plan for PSAP Call Handling System		X
Execute Beneficial Use (Go-Live) Milestone Acceptance Certificate(s).	X	X

3.7.3. Post-Migration Tasks

Post-Migration tasks include decommissioning and follow-up technical activities.

Tasks	MSCI	State of Nebraska
Perform system verification checks after each transition (9-1-1, Admin, hotlines, etc.).	X	
Initiate system monitoring and support.	X	
Address identified issues and concerns as they are found.	X	
Provide ongoing feedback to the MSCI team.		X
Decommission incumbent call routing service provider services after PSAP and carrier migration.		X
Decommission the legacy interfaces that terminate at the PSAP call-handling sites when the new NGCS routing service is delivering all 9-1-1 call traffic.		X

3.8. Project Finalization

Project finalization ensures that all final project completion criteria have been met. MSCI will conduct meetings to verify with the State of Nebraska that all contract deliverables have been satisfied. These meetings will allow the State of Nebraska an opportunity to discuss any final issues or address any questions associated with the closeout of System Implementation. MSCI will present the Final Project Acceptance certificate to the State of Nebraska when all contractual commitments of MSCI have been completed.

Tasks	MSCI	State of Nebraska
Resolve punch lists documented in order to meet all the criteria for final system acceptance.	X	
Assist MSCI with the resolution of identified punch list items by providing support, such as access to the sites, equipment, and system, and approval of the resolved punch list item(s).		X
Approve punch list resolution.		X
Provide As-built documentation to include, as applicable: • Policy Route Plan. • Escalation Process. • Circuit identification. • Failure Mitigation. • Network path diversity drawings into each PSAP. • Network path diversity drawings into each non-PSAP site or structure housing any element or device that is part of the overall system. • Call handling host / PSAP demarcation point drawings. • User interface training and reference materials.	X	
Review documentation with the Customer prior to the Customer's final acceptance of the drawings.	X	
Receive and approve all documentation provided by MSCI.		X
Execute Final Project Acceptance and Signature of Certificates.	X	X

Section 4

Training Structure

4.1.1. Training Methodology

End users will be trained in a virtual environment reflecting the 'go-live' environment using systems, applications, and hardware configured by and for the State of Nebraska and PSAPs. MSCI and State of Nebraska Project Managers are the coordinators of all classes based on the outline given in this document and based on the deployment schedule.

4.2. Training Plan Statement of Work

- MSCI will provide qualified Application Instructors required to fulfill course class counts and instructor-to-student ratios for delivery against the final agreed-upon training schedule.
- MSCI will provide experienced instructors with expert knowledge and previous experience teaching the application.
- If requested, MSCI will provide the instructors' resumes before the Instructor provides instruction to State of Nebraska and PSAP personnel.
- Instructors will maintain a positive learning environment, applying approved Instructor Protocols when necessary.
- Instructors will effectively manage teaching activities following the syllabus, ensuring all class parts are fully completed, including adequate time for hands-on practice and questions.

4.2.1. Instructor Responsibilities

Training Implementation

During State of Nebraska training program, the instructors will:

- Verify before class starts that all required User IDs and passwords are available for course participants, allowing the participants to access the systems and applications.
- Working with the MSCI and State of Nebraska implementation teams, verify that all equipment and software is available and working before the start of each class (e.g., applications, user login ids, passwords, etc.).
- Assign appropriate security roles and privileges to students so that all approved content and exercises may be taught during the course session.

- Ensure that data entry for practice work and training exercises is complete and ready for use during training.
- Reset passwords when required.
- Verify that all materials are available (Syllabus, Training Manuals, Quick Reference Cards, Attendance Sheets, Course Evaluations, and Training Certificates, if applicable).
- Inventory training materials for each class, ensuring enough materials are available for the number of students expected.
- Remove any testing or other data that negatively affects the training environment before the start of the class.

Instruction and Facilitation

This section outlines the MSCI Instructors' training, instruction, and facilitation duties. The instructors will:

- Understand the software and systems at an appropriate proficiency level.
- Ensure all participants have signed the training session attendance worksheet.
- Comfortably manage a class/webinar of up to 6 students (depending on the course).
- Ensure that all trainees can observe and participate.
- Teach the course in a logical manner, following the syllabus when applicable,, with adequate time for trainee practice and questions.
- Remain aware of the time allocated and ensure that all parts of the class are fully completed in the allotted time. All activities and exercises listed on the syllabus must be completed.
- Track all systems, applications, and hardware use and content issues.

Closing Activities

MSCI Instructors will:

- Distribute and collect training course evaluation forms for each trainee.
- Refresh the training environment for the next training class as required.
- Document and report any training issues that occurred during the session.

4.3. State of Nebraska and PSAP Responsibilities

Students are required to attend the entire duration of the course(s) and to participate in all hands-on activities. It is highly recommended that all students receive sufficient hands-on experience before the conclusion of the course.

This section outlines the duties of the State of Nebraska to facilitate successful training.

- Ensure State of Nebraska's and PSAP's Administrative Staff attend the MSCI Administrative training classes.
- Ensure State of Nebraska and PSAP:
 - Schedules personnel for the appropriate courses.

- Ensure training classes are fully staffed.
- Ensure students are prepared for the training.
- Ensure students are fully aware of operational policies; training will not cover any of the State of Nebraska or PSAP's policies or procedures.

Recommended Training Sessions			
Training Course	Description	Target Participants	Location
NGCS and ESInet (Done as a group of sessions on consecutive days)			
NGCS and ESInet Overview	An overview of the NGCS and ESInet, including admin training on routing rules, etc.	State of Nebraska and/or Regional Administrators and large PSAPs; recommended class size 8	One class included; location in the State of Nebraska to be determined by the State of Nebraska. Four-hour morning class
GIS Maintenance Tools	Reviews the functionality of the GIS Maintenance Toolset provided as an extension to ArcGIS.	GIS Administrators; recommended class size 8	Online
GIS Database Management and Spatial Interface	Covers uploading GIS data, managing discrepancies, and provisioning GIS data via Spatial Interface.	State of Nebraska and GIS Administrators; recommended class size 8	Online
Customer Web Portal	Provides an overview of Customer Web Portal features.	State of Nebraska and PSAP administration.	Online
Service Management			
NSOC / Service Management	This course provides an overview of our service offering and to open cases, change management, and the web portal.	State of Nebraska and/or Regional Administrators and large PSAPs; recommended class size 8	Done in conjunction with the NGCS and ESInet Overview. Four-hour afternoon class.
Location Database Training	This is primarily for administrative oversight of the services provided and assisting in discrepancy management.	All Database coordinators; recommended class size 10	Online
NGCS i3 Event Logger Training	Online webinar to provide overview of the operation of the i3 logger reporting web portal	State of Nebraska and PSAP administration.	Online

4.3.1. NGCS Routing Service & ESInet Overview

Description

The NGCS Routing Service & ESInet Overview course is designed for the administrators of a statewide, regional, or PSAP NGCS/ESInet. This class will provide an overview of the NGCS, the ESInet, the migration process, and the differences between legacy and NG9-1-1 call routing.

Delivery Method

- Lecture
- Presentation slides.

Prerequisites

- PSAP Operations Experience.

Equipment Needed

- Computer for review of presentation.

Training Content

This course typically occurs in advance of migration to the new Service:

- Introduction / Overview of NGCS.
- NGCS Operation.
- ESInet Overview.
- Overview of Routing Rules & Options.

Training Material

- Course Syllabus.
- Handouts (Routing Policy Summary).

4.3.2. NGCS GIS Tools and Procedures, Database Management Overview, Spatial Interface

Description

Training provides an introduction to GIS administrators an introduction to starting the data submission process, how to upload GIS data to the Spatial Interface, manage discrepancies identified during the Quality Control process, and provision GIS data into the NGCS Functional Elements (LVF/ECRF).

Delivery Method

- Self-paced web training

Prerequisites

- GIS Operation & Administration Experience.

Equipment Needed

- Computer for accessing web training.

Training Content

- Uploading GIS data.
- sFTP procedures for Data Submission.
- Data Requirements.
- Files, fields, format, content.
- Data Transformations (if necessary).
- Notification Configuration Options.
- Emails for data publishing confirmation.
- Emails for a blocked data publishing event.
- DataManager Website.
- Retrieval of QC reports.
- Definition and Interpretation of QC reports.
- A detailed description of each type of QC test.
- Typical errors that are reported.
- Review of specific examples.
- Suggestions for issue resolution.
- Creating layer and field mapping to the layers and data structure required by the LVF/ECRF.
- Status reporting.
- Map viewing.
- Exporting and downloading GIS data sets.
- Ongoing support for questions and additional training.

Training Material

- User Guides.
- Online training portal.

4.3.3. NGCS Location Database (LDB) Management

Description

This training provides agencies responsible for submitting data with an introduction to the data submission process. On-going training and support will be available as necessary. If necessary, one on one training can be scheduled with the LDB support staff.

A training website is included with videos that outline the LDB Manager Website's typical tasks.

Prerequisites

- GIS Operation & Administration Experience.

Delivery Method

- Self-paced web training.

Equipment Needed

- Computer for accessing web training.

Training Video Content

- Data submission, processing, and error workflows.
- Location Verification Function (LVF) reporting, searching, assignment, and discrepancy resolution.

Training Material

- Online training portal.

4.3.4. Customer Web Portal

Description

Training provides an overview of Customer Web Portal features. Features and data accessible is based upon individual permissions and user personas.

Delivery Method

- Lecture.
- Presentation slides.

Prerequisites

- PSAP Operations Experience.

Equipment Needed

- Computer for review of presentation.
- Computer for accessing web training.

Training Content

- CC Admin.
- Situational Awareness.
- Notifications.

- Internal Reports.
- External Reports.
- System Health.
- Service Performance.
- Service Reporting.
- Policy Configuration.
- Case Management.
- Dashboard.

Training Material

- User Guide.

DRAFT

Section 5

Support Plans

5.1.1. NSOC and Service Management

Description

The NGCS Support Plan - NSOC and Service Management are responsible for ensuring the customer has had a review of their Support Plan prior to Go - Live and Deployment

Delivery Method

- Online or In Person if CSM is doing this on-site.

Equipment Needed

- Computer for review of presentation.

Content

In advance of migration to the new Service, the CSM will cover the Support Plan:

- Introduction / Overview.
- NOC/SOC procedures.
- Escalations.
- Trouble Reporting/ Service Reporting.
- Service Management.
- Case Management.
- Change Management.
- Help Desk Portal.
- Executive Dashboard (Web Portal).
- Service Monitoring Tools.

Material

- Customer Support Plan
- User guide – Web Portal.

5.1.2. NGCS i3 Event Logger

Description

These courses include reviewing i3 logging reports and describing how to access data and run reports.

Prerequisites

- PSAP Operations Experience.

Training Content

- Report rendering and generation interface.
- Standard reports overview and features.
- Ad-Hoc reports.

Training Material

- User Guides.

DRAFT

Section 6

PSAP Acceptance Test Plan

6.1. Purpose

The Acceptance Test Plan will be customized to address each PSAP as required. The test plans will be very similar in their outline, criteria, and execution, but will differ in their testing of the applicable call routing destinations and transfers.

The MSCI Next Generation Core Services (NGCS) provides location and call routing functionalities. The call routing service provides integration of next-generation technologies for emergency call traffic routing to Public Safety Answering Points (PSAPs). This test plan supports the quality assurance processes used to ensure that the implementation of the service for a new PSAP meets the expected functional requirements of the customer and MSCI. The objective is to validate effective 9-1-1 call delivery functionality. The pass/fail criteria are determined by the verification of expected results within a test case.

6.1.1. Scope

This NGCS testing is a verification of call routing and location information functionality with the PSAP prior to migration. Testing is conducted remotely and/or on-site at the customer's location. Testing may incorporate manual and automated test methods. Completion of the testing will result in a written report issued by MCSI. The test report will be a summary of the test results with confirmation of meeting functional and operational criteria.

The tests that will be performed are listed below and described in more detail throughout this section.

- ESInet Edge Router / Physical Connectivity Test
- NGCS Configuration (Router) Test
- Network Conference Test
- Preliminary Test
- Location Service Test
- Location Service Delivery Test
- Wireline Call Test
- No Record Found Wireline Call Test Call
- Wireless Call Test
- Text to 9-1-1 Test (if applicable)

- Conference Call Tests
- 10-Digit PSTN Conference Call Tests
- Policy Rules (Overflow / Next Hop) Test
- Error Code Route Tests
- Abandoned State Route Test

6.2. Prerequisites

All CHSs must be in a service readiness state; all hardware, software, and networking configurations must be complete prior to any testing. Any third party systems that ingest location data (ALI spill) from the CHS must likewise be ready. Specific test elements that reference third-party systems such as CAD, logging recorders, and mapping are **not used to determine whether the test case passes or not**; they are informational only and are designed to help the specific PSAP identify issues that must be addressed. **Only those test elements within MSCI's scope are used to determine whether a given test case passes or fails.**

Acceptance testing occurs after MSCI has successfully completed NGCS service readiness testing.

6.3. Demarcation Point Verification

The MSCI NGCS Service ESInet is extended to each relevant call handling system host location. The MSCI NGCS Service demarcation points are defined as the following:

- A physical female port on the MSCI ESInet edge router

Two MSCI ESInet edge routers will be placed at each relevant call handling host location.

- NGCS Edge Router Test Case

6.3.1. ESInet Edge Router / Physical Connectivity

Two MSCI ESInet edge routers will be placed at each relevant call handling host location. Each of their physical connectivity will be verified and detailed.

6.4. MSCI NGCS Service Configuration - Customer Specific

6.4.1. MSCI NGCS Configuration

The MSCI NGCS service utilizes Universal Resource Identifiers (URI) for each destination that calls can be routed and/ or transferred to. The URI and policy route plan (aka call flow strategy) lists each of the

destination URIs that will be configured in the MSCI NGCS service. Each URI will be verified for proper configuration within the MSCI NGCS service. This will be achieved by MSCI verifying that the documented policy route plan matches the configuration in the system.

6.4.2. Conference / Transfer Function

A network conference allows the call taker to add a third party to an existing 9-1-1 call, for the purpose of call conferencing and/or attended call transfer. The CHS can achieve this by sending a conference or transfer request to the MSCI NGCS service. MSCI will verify the proper functioning of each conference/transfer destination within the MSCI NGCS service.

6.5. Pre-Test System Observations

Before the acceptance test can be executed, it is important to establish a benchmark of the system's status. This test case will verify that the CHS is working correctly before exercising any changes in the system regarding MSCI Location Services. The CHS will be considered to work correctly if it meets all of the expected results listed in the test case below. An answered call(s) will be observed to ensure quality two-way audio, call control is working accurately, and caller location is received by the CHS. The customer's representative will be consulted to verify these results within the respective CHS system.

Multiple calls will be observed to verify baseline operation of the incumbent call routing and call handling system.

6.6. Location Service Testing

MSCI Location Services testing focuses on the request of, delivery, redundancy, and formatting of the location information for emergency calls. The test cases verify the LDB configuration, location information delivery to the CHS (manual and automatic), location information formatting within the CHS, and the ability to receive updates across the duration of a call. The customer will be able to utilize requests and responses for ALI, view logs, do imports and exports, modify records, and run reports. Interoperability testing with the CHS includes:

- Verify ANI/ALI receipt payload and format
- Verify ANI/ALI auto-update
- Verify ANI/ALI manual update

Depending upon how the end customer manages the NGCS and associated location database, these tests may be performed at an enterprise level with the system administrator over a regional program and/or at the individual local jurisdiction level per customer of record discretion.

6.7. Location Database Service Testing

The existing ALI and MSAG records will be extracted from the incumbent ALI service providers system, properly formatted, and imported into the MSCI NGCS service. Any records found to have errors will undergo examination and correction. During the conversion, each OSP will deliver service orders to both the incumbent ALI service and the MSCI NGCS service prior to cut over.

6.8. Wireline Test Call

To validate the CHS against MSCI NGCS, the system needs to be exercised by sending in multiple calls, simultaneously at times, and verifying that all of the routing is successful to all locations, for all endpoints, and for all PSAPs. Additionally, the error conditions need to be validated for each call flow scenario. Finally, failure testing should ensure that resiliency is achieved throughout the system and in case of component or service failure.

A wireline test call will be placed to PSAPs to verify quality, accuracy, and completeness.

Operational testing will be performed to determine that all 9-1-1 calls:

- Are delivered to the correct PSAP location
- Contain the correct additional information
- Meet public safety voice quality standards
- Route correctly based upon routing configurations and conditions

6.9. No Record Found Wireline Test Call

To validate the CHS with the MSCI NGCS Service, the system needs to be exercised by sending in multiple calls, simultaneously at times, and verifying that all of the routing is successful to all locations, for all endpoints, and for all PSAPs. Additionally, the error conditions need to be validated for each call flow scenario. Finally, failure testing should be done to ensure that resiliency is being achieved throughout the system and in case of component or service failure.

Operational testing will be performed to determine that all 9-1-1 calls:

- Are delivered to the correct PSAP location
- Contain the correct additional information
- Meet public safety voice quality standards

A wireline test call will be placed to PSAPs to verify quality, accuracy, and completeness.

6.10. Wireless Test Call

To validate the CHS with the MSCI NGCS Service, the system needs to be exercised by sending in multiple calls, simultaneously at times, and verifying that all of the routing is successful to all locations, for all endpoints, and for all PSAPs. Additionally, the error conditions need to be validated for each call flow scenario. Finally, failure testing should be done to ensure that resiliency is being achieved throughout the system and in case of component or service failure.

A wireless test call will be placed to PSAPs to verify quality, accuracy, and completeness.

Operational testing will be performed to determine that all 9-1-1 calls:

- Are delivered to the correct PSAP location
- Contain the correct additional information
- Meet public safety voice quality standards
- Route correctly based upon routing configurations and conditions

6.11. 10-Digit PSTN Test Call

If applicable, a test call will be initiated to a PSAP and transferred to a 10-digit PSTN to verify quality, accuracy, and completeness. This tests an initial call from the CHS to the MSCI NGCS, to a PSTN endpoint.

6.12. Conference Bridge and NGCS Transfer Testing

MSCI NGCS supports network conferences of two or more parties. Network conferences can be to destinations using Emergency Call Handling (ECH) systems or PSTN. The network conference sends an invite to the endpoint or gateway, allowing them to join the in-progress call. It also allows parties to leave the conference without affecting the remaining participants. Endpoints will verify audio and data (as applicable) to verify quality, accuracy, and functionality.

The CHS will execute a test for a conference call/transfer via MSCI NGCS. This will validate that the data sent by the CHS is properly formatted and that the functionality is available.

6.13. Ring No Answer Call Routing

When a valid 9-1-1 call reaches its destination endpoint and the call is not serviced within the agreed upon timeframe with the customer it will cause an Overflow / Next Hop condition. This configuration is used to send the call to a different location to be answered. The Overflow / Next Hop route is unique in that the CHS does not need to respond with a SIP response code. The Overflow / Next Hop routing

occurs based on a timer within the NGCS Call Routing Service. Once that time elapses, the behavior is invoked and the call gets sent to the new location.

6.14. Error Code Call Routing

MSCI NGCS will invoke the error code route when it receives a SIP error response code of any type. Some examples of situations that may cause a call to be rejected are: A) all call takers are on a call, B) no call takers are available to take a call but are logged on, or C) all call takers are logged out of a system. These tests simulate the situation and test the appropriate routing determination and execution.

6.15. Abandoned State Routing

MSCI NGCS delivers calls to an entity (e.g., PSAP) based upon its assigned URI. MSCI NGCS can pre-program an Abandoned State URI to point to a different entity that can be enabled or disabled. This alternate entity destination is used in cases where the original entity is offline due to planned (e.g., maintenance) or unplanned (e.g., evacuation) events. Some reasons for the use of abandoned state include building renovations, a maintenance window, loss of power for an extended duration, or other natural disaster that no longer allows call taking to occur at the PSAP.

Section 7

Project Finalization

Project finalization ensures that all final project completion criteria have been met. MSCI will conduct meetings to verify with the State of Nebraska that all contract deliverables have been satisfied. These meetings will allow the State of Nebraska an opportunity to discuss any final issues or address any questions associated with the closeout of System Implementation. MSCI will present the Final Project Acceptance certificate to the State of Nebraska when all contractual commitments of MSCI have been completed.

Tasks	MSCI	State of Nebraska
Resolve punch lists documented in order to meet all the criteria for final system acceptance.	X	
Assist MSCI with the resolution of identified punch list items by providing support, such as access to the sites, equipment, and system, and approval of the resolved punch list item(s).		X
Approve punch list resolution.		X
Provide As-built documentation to include, as applicable: • Policy Route Plan. • Escalation Process. • Circuit identification. • Failure Mitigation. • Network path diversity drawings into each PSAP. • Network path diversity drawings into each non-PSAP site or structure housing any element or device that is part of the overall system. • Call handling host / PSAP demarcation point drawings. • User interface training and reference materials.	X	
Review documentation with the Customer prior to the Customer's final acceptance of the drawings.	X	
Receive and approve all documentation provided by MSCI.		X

Tasks	MSCI	State of Nebraska
Execute Final Project Acceptance and Signature of Certificates.	X	X

Thank you for choosing Motorola Solutions Connectivity, Inc.

DRAFT

Exhibit 5 Sample Project Schedule

Nebraska Sample Project Schedule



	Task Name	Duration	Plan Start	Plan Finish	Predecessors	Assigned To
1	Nebraska NGCS Call Routing Service Project	581d	07/01/26	10/02/28		
2	Award	35d	07/01/26	08/19/26		
3	Contract Date {Contract Signing S2S}	0	07/01/26	07/01/26		Shared
4	Customer Kick Off Meeting {S2S}	1d	08/11/26	08/11/26	3FS +28d	MSCI
5	Design Review {S2S}	5d	08/12/26	08/18/26	4	Shared
6	Project Management Plan	~0	08/19/26	08/19/26	5	MSCI
7	Preliminary Project Schedule	0	08/19/26	08/19/26	6	Shared
8	Letter of Agency	0	08/17/26	08/17/26	4FS +4d	Customer
9	Notice to Proceed	0	08/19/26	08/19/26	6, 8	Customer
10	PSAP Data Gathering & Transition Strategy Refinement	30d	08/12/26	09/23/26		
11	PSAP Data Gathering	30d	08/12/26	09/23/26	4	Shared
12	Transition Strategy Refinement	30d	08/12/26	09/23/26	4	Shared
13	PSAP Data Gathering & Transition Strategy Complete	0	09/23/26	09/23/26	11, 12	Shared
14	Procurement	291d	08/12/26	10/01/27		
15	Hardware Procurement	110d	08/12/26	01/21/27	4	MSCI
16	Ingress Network Order/Build	90d	08/20/26	01/01/27	9	MSCI
17	Egress Network Order/Build	270d	09/11/26	10/01/27	9FS +15d	MSCI
96	Procurement Phase Complete	0	10/01/27	10/01/27	15, 16, 17	MSCI
97	Ingress Network Build	251d	09/18/26	09/13/27		
98	OSP Outreach	100d	09/18/26	02/12/27	9FS +20d	MSCI
99	Split Exchange Analysis	100d	10/09/26	03/05/27	98SS +15d	MSCI
100	Network Data Collection	40d	02/15/27	04/09/27	98	MSCI
101	Network Build / POI	120d	01/04/27	06/18/27	16	MSCI
102	Testing Ingress Test & Turn Up	30d	01/04/27	02/12/27	16	MSCI
103	Testing Ingress Build Complete	0	02/12/27	02/12/27	102	MSCI
104	Production Ingress Test & Turn Up	60d	06/21/27	09/10/27	101	MSCI
105	Production Ingress Build Complete	0	09/13/27	09/13/27	104FS +1d	MSCI
106	ESInet Edge Appliance Configuration & Installs	191d	01/22/27	10/15/27		
107	Receive & Stage ESInet Edge Appliances	30d	01/22/27	03/04/27	15	MSCI
108	Configure and Install ESInet Edge Appliances	190d	01/25/27	10/15/27		MSCI
109	PSAP Group 1	30d	01/25/27	03/05/27		MSCI
110	Grand Island/Hall County Communications	30d	01/25/27	03/05/27	19	MSCI
111	Grand Island/Hall County Emergency Management	30d	01/25/27	03/05/27	19	MSCI
112	Boone County Sheriff	30d	01/25/27	03/05/27	19	MSCI
113	Butler County Sheriff	30d	01/25/27	03/05/27	19	MSCI
114	Custer County	30d	01/25/27	03/05/27	19	MSCI
115	Hamilton County Sheriff	30d	01/25/27	03/05/27	19	MSCI
116	Columbus-Platte County Joint Comm Center	30d	01/25/27	03/05/27	19	MSCI
117	Region 26 Council EMA & 911 Center	30d	01/25/27	03/05/27	19	MSCI
118	Saunders County	30d	01/25/27	03/05/27	19	MSCI
119	PSAP Group 2	30d	03/08/27	04/16/27		MSCI
120	Norfolk Police Departmennt	30d	03/08/27	04/16/27	29	MSCI
121	Dakota County Communications	30d	03/08/27	04/16/27	29	MSCI
122	Cedar County Emergency Management	30d	03/08/27	04/16/27	29	MSCI
123	Dixon County Sheriff	30d	03/08/27	04/16/27	29	MSCI
124	Knox County Sheriff	30d	03/08/27	04/16/27	29	MSCI
125	Thurston County Sheriff	30d	03/08/27	04/16/27	29	MSCI

	Task Name	Duration	Plan Start	Plan Finish	Predecessors	Assigned To
126	Wayne Police Department	30d	03/08/27	04/16/27	29	MSCI
127	Pierce County Sheriff	30d	03/08/27	04/16/27	29	MSCI
128	 PSAP Group 3	84d	05/31/27	09/23/27		MSCI
129	Antelope County	84d	05/31/27	09/23/27	38	MSCI
130	Brown County Sheriff	84d	05/31/27	09/23/27	38	MSCI
131	Cherry County Sheriff	84d	05/31/27	09/23/27	38	MSCI
132	Boyd-Holt Counties Joint E911	84d	05/31/27	09/23/27	38	MSCI
133	Rock County Sheriff	84d	05/31/27	09/23/27	38	MSCI
134	Sheridan County Sheriff	84d	05/31/27	09/23/27	38	MSCI
135	Adams County Sheriff/City of Hastings	84d	05/31/27	09/23/27	38	MSCI
136	Cass County	84d	05/31/27	09/23/27	38	MSCI
137	Clay County	84d	05/31/27	09/23/27	38	MSCI
138	Fiillmore County	84d	05/31/27	09/23/27	38	MSCI
139	Gage County/City of Beatrice	84d	05/31/27	09/23/27	38	MSCI
140	Jefferson County	84d	05/31/27	09/23/27	38	MSCI
141	Johnson County	84d	05/31/27	09/23/27	38	MSCI
142	Lancaster County Fire	84d	05/31/27	09/23/27	38	MSCI
143	Lancaster County PD	84d	05/31/27	09/23/27	38	MSCI
144	Nemaha County	84d	05/31/27	09/23/27	38	MSCI
145	Nuckolls County	84d	05/31/27	09/23/27	38	MSCI
146	Otoe County	84d	05/31/27	09/23/27	38	MSCI
147	Richardson County/City of Falls City	84d	05/31/27	09/23/27	38	MSCI
148	Saline County Sheriff	84d	05/31/27	09/23/27	38	MSCI
149	Seward County	84d	05/31/27	09/23/27	38	MSCI
150	Thayer County Sheriff	84d	05/31/27	09/23/27	38	MSCI
151	Webster County Sheriff	84d	05/31/27	09/23/27	38	MSCI
152	York County Communications	84d	05/31/27	09/23/27	38	MSCI
153	 PSAP Group 4	10d	05/31/27	06/11/27		MSCI
154	Fremont Dodge County Sheriff (Dodge Viper)	10d	05/31/27	06/11/27	63	MSCI
155	Burt County Sheriff (Dodge Viper)	10d	05/31/27	06/11/27	63	MSCI
156	Colfax County Sheriff (Dodge Viper)	10d	05/31/27	06/11/27	63	MSCI
157	Cuming County (Dodge Viper)	10d	05/31/27	06/11/27	63	MSCI
158	 PSAP Group 5	5d	07/12/27	07/16/27		MSCI
159	Douglas County	5d	07/12/27	07/16/27	68	MSCI
160	Sarpy County	5d	07/12/27	07/16/27	68	MSCI
161	Washington County	5d	07/12/27	07/16/27	68	MSCI
162	 PSAP Group 6	30d	08/23/27	10/01/27		MSCI
163	Buffalo County	30d	08/23/27	10/01/27	72	MSCI
164	Chadron Police Department	30d	08/23/27	10/01/27	72	MSCI
165	Chase County Sheriff	30d	08/23/27	10/01/27	72	MSCI
166	Cheyenne County	30d	08/23/27	10/01/27	72	MSCI
167	Furnas County	30d	08/23/27	10/01/27	72	MSCI
168	Garden County	30d	08/23/27	10/01/27	72	MSCI
169	Holdrege Police Department	30d	08/23/27	10/01/27	72	MSCI
170	Kearney County Sheriff	30d	08/23/27	10/01/27	72	MSCI
171	Keith County	30d	08/23/27	10/01/27	72	MSCI
172	Kimball County	30d	08/23/27	10/01/27	72	MSCI
173	Perkins County Sheriff	30d	08/23/27	10/01/27	72	MSCI
174	Red Willow/City of McCook	30d	08/23/27	10/01/27	72	MSCI
175	Howard County	30d	08/23/27	10/01/27	72	MSCI

	Task Name	Duration	Plan Start	Plan Finish	Predecessors	Assigned To
176	Dawson County	30d	08/23/27	10/01/27	72	MSCI
177	 PSAP Group 7	10d	10/04/27	10/15/27		MSCI
178	Dundy County	10d	10/04/27	10/15/27	87	MSCI
179	Franklin County Sheriff	10d	10/04/27	10/15/27	87	MSCI
180	Hitchcock County	10d	10/04/27	10/15/27	87	MSCI
181	Morrill County Sheriff	10d	10/04/27	10/15/27	87	MSCI
182	Scotts Bluff County Communications	10d	10/04/27	10/15/27	87	MSCI
183	 PSAP Group 8	5d	10/04/27	10/08/27		
184	Box Butte County Sheriff	5d	10/04/27	10/08/27	93	MSCI
185	North Platte Police Department	5d	10/04/27	10/08/27	93	MSCI
186	 Location Services (LDB & GIS)	342d	09/03/26	01/04/28		
187	 Project Initiation	225d	09/03/26	07/23/27		MSCI
188	Kickoff	1d	05/03/27	05/03/27	205FS -175d	MSCI
189	 Data Collection	225d	09/03/26	07/23/27		MSCI
190	MSAG & ALI Data from Outgoing Provider	60d	09/03/26	12/02/26	9FS +10d	MSCI
191	GIS Data	60d	05/03/27	07/23/27	188SS	Customer
192	Collaborative Review	1d	05/03/27	05/03/27	188SS	Shared
193	 Spatial Data Readiness	101d	04/06/27	08/24/27		MSCI
194	Data Compliance Checkpoint #2	1d	08/11/27	08/11/27	240SS -24d	MSCI
195	Unified GIS (Training)	13d	04/06/27	04/22/27	192FS -20d	MSCI
196	Final GIS Data Review	1d	08/13/27	08/13/27	200SS -7d	MSCI
197	Geoprocessing Toolkit (Training)	33d	04/06/27	05/20/27	192FS -20d	MSCI
198	Submit MOP for CAB Approval	1d	08/24/27	08/24/27	240SS -15d	MSCI
199	CAB Approval Received	1d	08/24/27	08/24/27	240SS -15d	MSCI
200	GIS Data Import to ECRF	1d	08/24/27	08/24/27	240SS -15d	MSCI
201	 Legacy Data Readiness	75d	09/22/27	01/04/28		MSCI
202	Buffer Area LOAs Received	1d	09/22/27	09/22/27	204SS -60d	MSCI
203	All Data Elements to Data Services	1d	11/03/27	11/03/27	204SS -30d	MSCI
204	Go / No Go Meeting (MSAG/ALI Production Loads)	1d	12/15/27	12/15/27	205SS -12d	MSCI
205	MSAG Load	1d	12/31/27	12/31/27	206SS -2d	MSCI
206	ALI Load	1d	01/04/28	01/04/28		MSCI
207	Dual Provisioning Starts	0	01/04/28	01/04/28	206	MSCI
208	 MSCI Router Integration	523d	08/12/26	08/22/28		
209	 Call Flow Design	110d	08/12/26	01/21/27		
210	Call Flow Design Analysis / Training Prep	30d	08/12/26	09/23/26	4	Shared
211	 Call Flow Workshops	75d	10/01/26	01/21/27		Shared
212	PSAP Group 1	5d	10/01/26	10/07/26	210FS +5d	Shared
213	PSAP Group 2	5d	10/16/26	10/22/26	212FS +5d	Shared
214	PSAP Group 3	5d	10/30/26	11/05/26	213FS +5d	Shared
215	PSAP Group 4	5d	11/16/26	11/20/26	214FS +5d	Shared
216	PSAP Group 5	5d	12/02/26	12/08/26	215FS +5d	Shared
217	PSAP Group 6	5d	12/16/26	12/22/26	216FS +5d	Shared
218	PSAP Group 7	5d	01/01/27	01/07/27	217FS +5d	Shared
219	PSAP Group 8	5d	01/15/27	01/21/27	218FS +5d	Shared
220	Call Flow Design Complete	0	01/21/27	01/21/27	211	Shared
221	 ESInet Activation & Testing	190d	01/25/27	10/15/27		
222	PSAP Group 1	30d	01/25/27	03/05/27	109FF	MSCI
223	PSAP Group 2	30d	03/08/27	04/16/27	119FF	MSCI
224	PSAP Group 3	84d	05/31/27	09/23/27	128FF	MSCI
225	PSAP Group 4	10d	05/31/27	06/11/27	153FF	MSCI

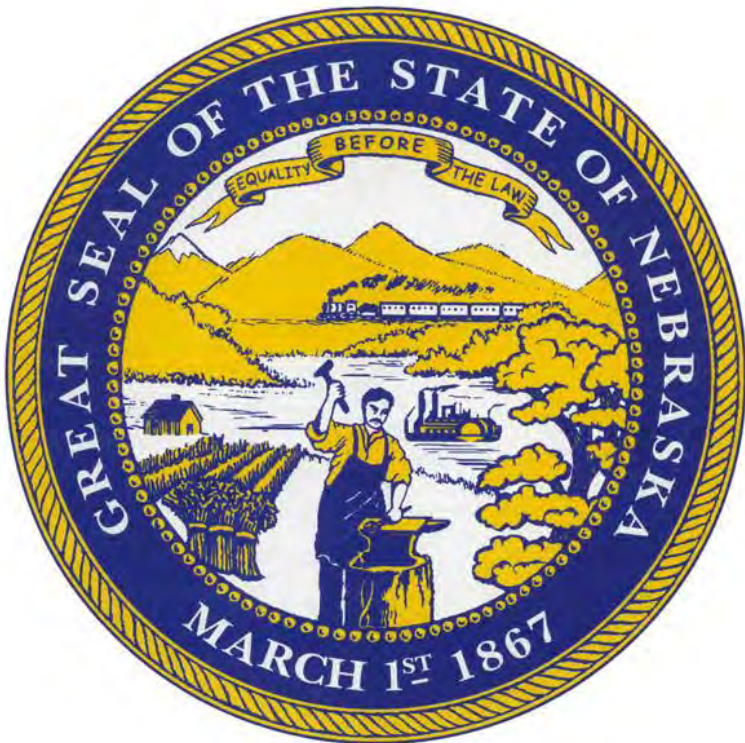
	Task Name	Duration	Plan Start	Plan Finish	Predecessors	Assigned To
226	PSAP Group 5	5d	07/12/27	07/16/27	158FF	MSCI
227	PSAP Group 6	30d	08/23/27	10/01/27	162FF	MSCI
228	PSAP Group 7	10d	10/04/27	10/15/27	177FF	MSCI
229	PSAP Group 8	5d	10/04/27	10/08/27	183FF	MSCI
230	Core Install & Test Complete	0	10/15/27	10/15/27	222, 223, 224, 225,	Shared
231	 Policy Loading & Call Flow	191d	01/22/27	10/15/27		
232	MSCI Router Ready to Load Policy Route Plan	1d	01/22/27	01/22/27	5, 220	
233	Load PSAP Call Routing Policies	15d	08/24/27	09/13/27	240SS -15d	MSCI
234	NG911 Router Integration Complete	0	10/15/27	10/15/27	232, 233, 230	MSCI
235	 Testing & Validation	387d	08/12/26	02/14/28		
236	 Call Handling System Interoperability Testing (IOT)	60d	08/12/26	11/05/26		MSCI / CHS Vendor
237	Zetron	60d	08/12/26	11/05/26	4	MSCI / CHS Vendor
238	Solacom	60d	08/12/26	11/05/26	4	MSCI / CHS Vendor
239	Other (?) note: NPQ shows an unknown on a site, placeholder to update	60d	08/12/26	11/05/26	4	MSCI / CHS Vendor
240	 NGCS Core Testing & Validation	95d	09/14/27	01/24/28		MSCI
241	PSAP Group 1	15d	09/14/27	10/04/27	105, 212, 222	MSCI
242	PSAP Group 2	10d	10/05/27	10/18/27	241, 213, 223	MSCI
243	PSAP Group 3	30d	10/19/27	11/29/27	242, 214, 224	MSCI
244	PSAP Group 4	10d	11/30/27	12/13/27	243, 215, 225	MSCI
245	PSAP Group 5	5d	12/14/27	12/20/27	244, 216, 226	MSCI
246	PSAP Group 6	15d	12/21/27	01/10/28	245, 217, 227	MSCI
247	PSAP Group 7	5d	01/11/28	01/17/28	246, 218, 228	MSCI
248	PSAP Group 8	5d	01/18/28	01/24/28	247, 219, 229	MSCI
249	 NGCS Functional Testing & Validation	90d	10/05/27	02/07/28		MSCI
250	PSAP Group 1	10d	10/05/27	10/18/27	241, 263	MSCI
251	PSAP Group 2	10d	10/19/27	11/01/27	242, 264	MSCI
252	PSAP Group 3	10d	11/30/27	12/13/27	243, 265	MSCI
253	PSAP Group 4	10d	12/14/27	12/27/27	244, 266	MSCI
254	PSAP Group 5	10d	12/21/27	01/03/28	245, 267	MSCI
255	PSAP Group 6	10d	01/11/28	01/24/28	246, 268	MSCI
256	PSAP Group 7	10d	01/18/28	01/31/28	247, 269	MSCI
257	PSAP Group 8	10d	01/25/28	02/07/28	248, 270	MSCI
258	NextGen Router Production Ready	0	02/14/28	02/14/28	249FS +5d	MSCI
259	 Migration Planning	341d	09/03/26	01/03/28		
260	LSR Transition Agreement	~0	04/09/27	04/09/27	9SS +160d	Shared
261	Call Handling System Release Upgrades by Customer	150d	09/03/26	04/09/27	260FF	Customer
262	 Call Handling System Configurations by Customer	95d	08/24/27	01/03/28		Customer
263	Group 1	15d	08/24/27	09/13/27	241SS -15d	Customer
264	Group 2	10d	09/14/27	09/27/27	242SS -15d	Customer
265	Group 3	30d	09/28/27	11/08/27	243SS -15d	Customer
266	Group 4	10d	11/09/27	11/22/27	244SS -15d	Customer
267	Group 5	5d	11/23/27	11/29/27	245SS -15d	Customer
268	Group 6	15d	11/30/27	12/20/27	246SS -15d	Customer
269	Group 7	5d	12/21/27	12/27/27	247SS -15d	Customer
270	Group 8	5d	12/28/27	01/03/28	248SS -15d	Customer
271	ALL Customer Call Handling Systems Ready	0	01/03/28	01/03/28	262	Customer
272	 Monitor & Support	30d	01/03/28	02/14/28		
273	Monitoring Activation	10d	01/31/28	02/14/28	258SF	MSCI
274	Design Documentation	30d	01/03/28	02/14/28	273FF	MSCI
275	Readiness Review	0	02/14/28	02/14/28	273, 274	MSCI

	Task Name	Duration	Plan Start	Plan Finish	Predecessors	Assigned To
276	NSOC Activation Complete	0	02/14/28	02/14/28	275	MSCI
277	 MSCI Location Services (LDB) Migration	165d	01/05/28	08/22/28		
278	LDB Operational / Production Ready	1d	01/05/28	01/05/28	207	Shared
279	End Dual Provisioning	0	08/22/28	08/22/28	289FS +10d	MSCI
280	LDB Migration Complete	0	08/22/28	08/22/28	279	Shared
281	 MSCI Router (Voice) Migration	4d	02/14/28	02/18/28		
282	Acceptance Test Plans Completed/Approved	1d	02/14/28	02/15/28	258SS	Shared
283	Voice Migration Complete	0	02/18/28	02/18/28	282FS +3d	Shared
284	Go Live Milestone S2S	0	02/18/28	02/18/28	283	Shared
285	 Legacy Router / OSP Migration	131d	02/21/28	08/22/28		
286	Dual-Mode Router Period	20w	02/21/28	07/10/28	287SS	Shared
287	OSP Migration Period	120d	02/21/28	08/07/28	284FS +1d	MSCI
288	Disconnect Legacy Selective Routers	0	08/22/28	08/22/28	289FS +2w	Customer
289	OSP Migration Complete	0	08/08/28	08/08/28	287FS +1d	MSCI
290	 i3 Logging/Reporting, Customer Web Portal	162d	11/30/27	07/12/28		
291	Collect Customer Information	10d	11/30/27	12/13/27	249FF -40d	Customer
292	Complete New PSAPs Data Collection Form	10d	11/30/27	12/13/27	291SS	MSCI
293	Complete Customer Web Portal Configuration Worksheet	10d	12/14/27	12/27/27	291	MSCI
294	Complete i3 Logger Data Collection Worksheet	10d	01/18/28	02/01/28	282FS -20d	MSCI
295	Configure Customer Web Portal	10d	06/13/28	06/26/28	293FS +120d	MSCI
296	Customer Web Portal Training	10d	06/29/28	07/12/28	295FS +2d	Shared
297	Customer Web Portal Live	0	07/12/28	07/12/28	296	MSCI
298	Configure i3 Logger	25d	02/01/28	03/07/28	294	MSCI
299	i3 Logger Report Training	5d	03/07/28	03/14/28	298	Shared
300	i3 Logger Reporting Live	0	03/14/28	03/14/28	299	MSCI
301	i3 Logger and Customer Web Portal Live	0	07/12/28	07/12/28	297, 300	MSCI
302	 Project Close-Out / Operations	161d	02/18/28	10/02/28		
303	Handover to Operations {Handover to Support S2S}	1d	02/18/28	02/21/28	283	MSCI
304	Punch List Resolution	20d	08/07/28	09/04/28	286, 287	MSCI
305	Final Documentation	20d	09/04/28	10/02/28	304	MSCI
306	Project Finish {Final Acceptance S2S}	0	10/02/28	10/02/28	289, 305	Shared
307						
308						
309						
310						
311						
312						
313						
314						
315						
316						

Exhibit 6 Architecture and Topology Diagrams

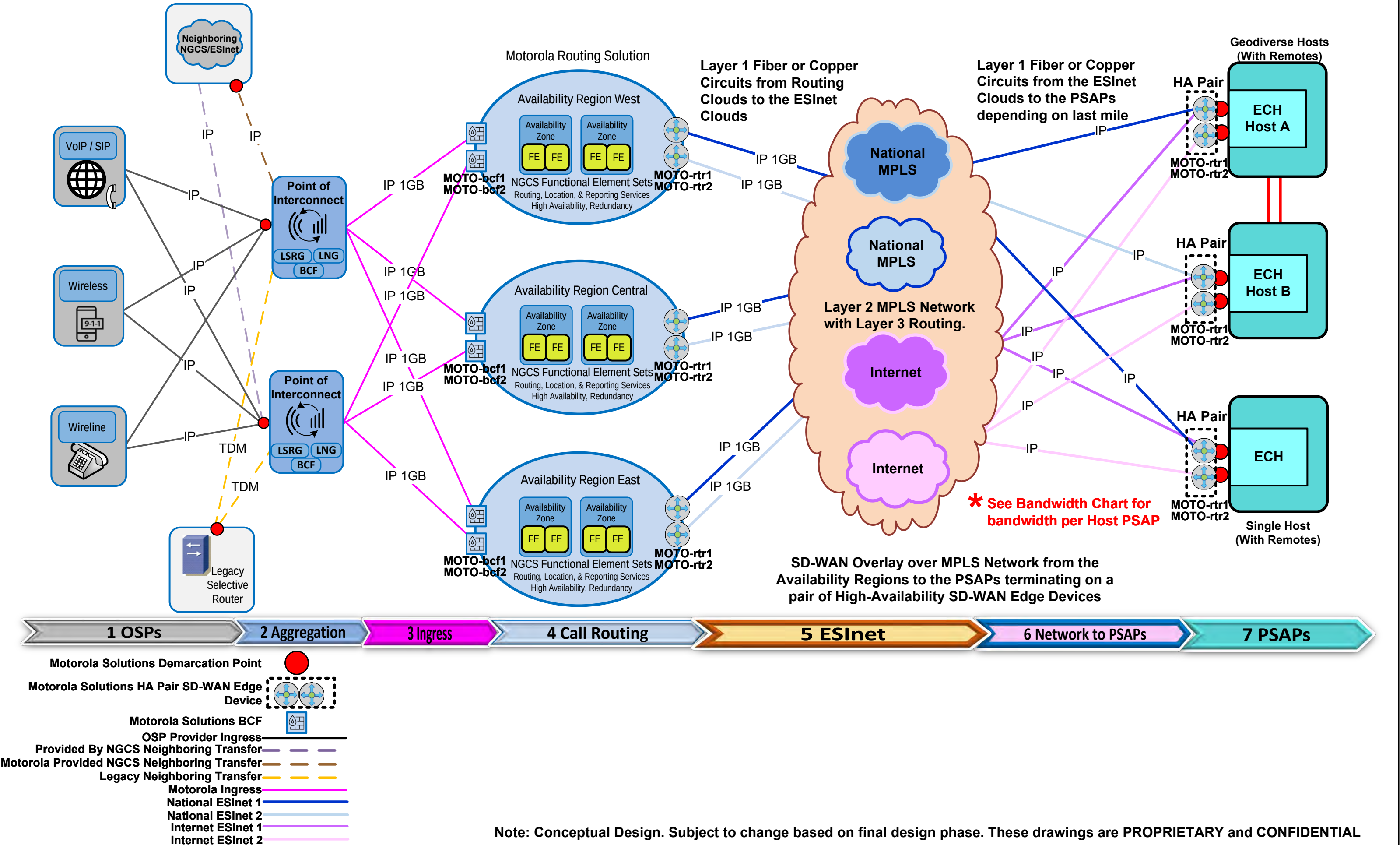
State of Nebraska

Network Configuration Document State of Nebraska

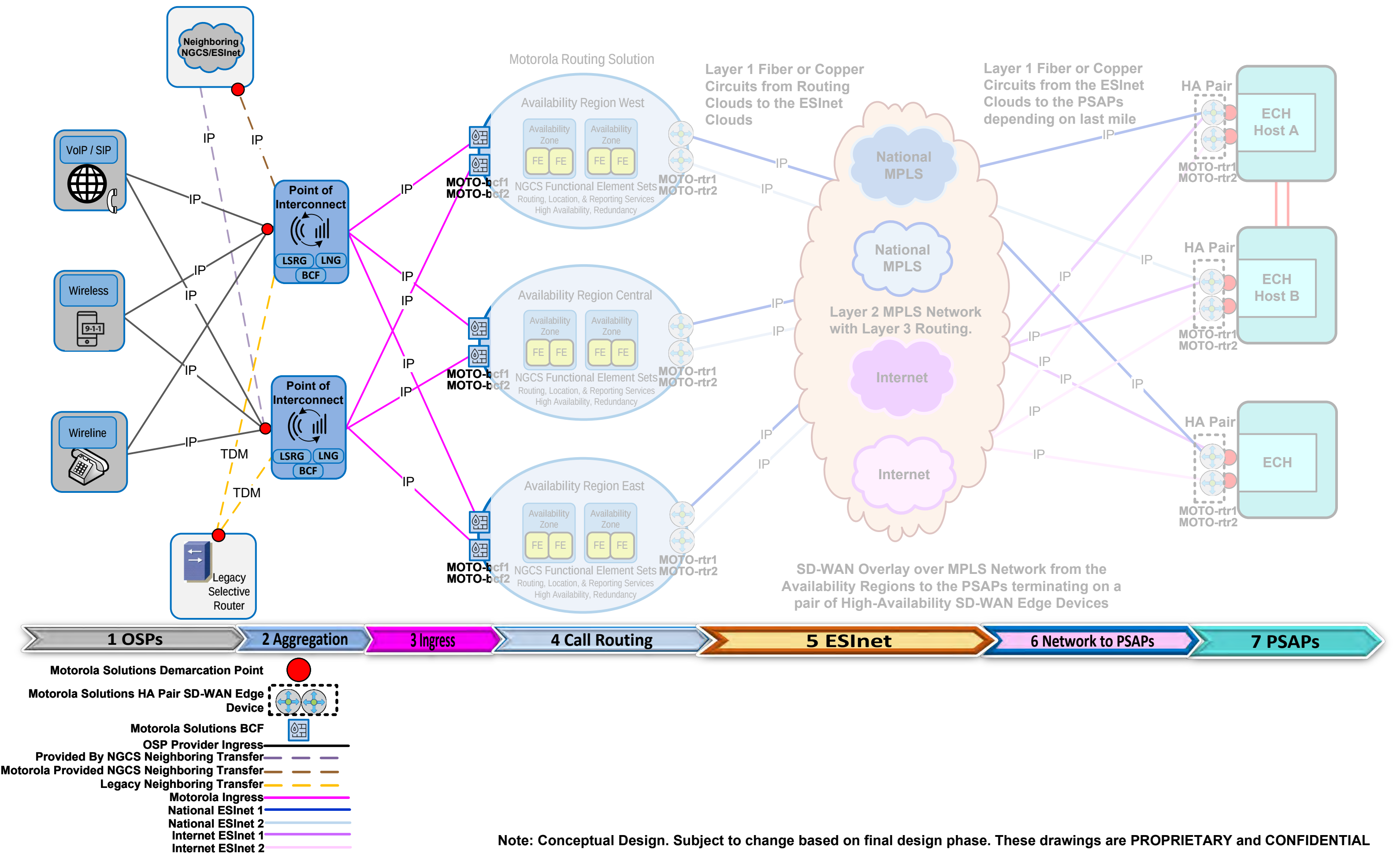


Assumptions / Notes / Purpose:	Legend	Title: State of Nebraska – NGCS High Level Design	
		Project: State of Nebraska 2026 RFP	
		Version: 4.03242026	Date: March 24, 2026
		☒ Preliminary ☐ Final	
		Filename: Visio_NGCS_IP Circuits_ ESInet_State of Nebraska VESTA NXT Router v4.03242026.vsd	
		Sr. Architect: Steven Ferraro	Page: 1 of 8

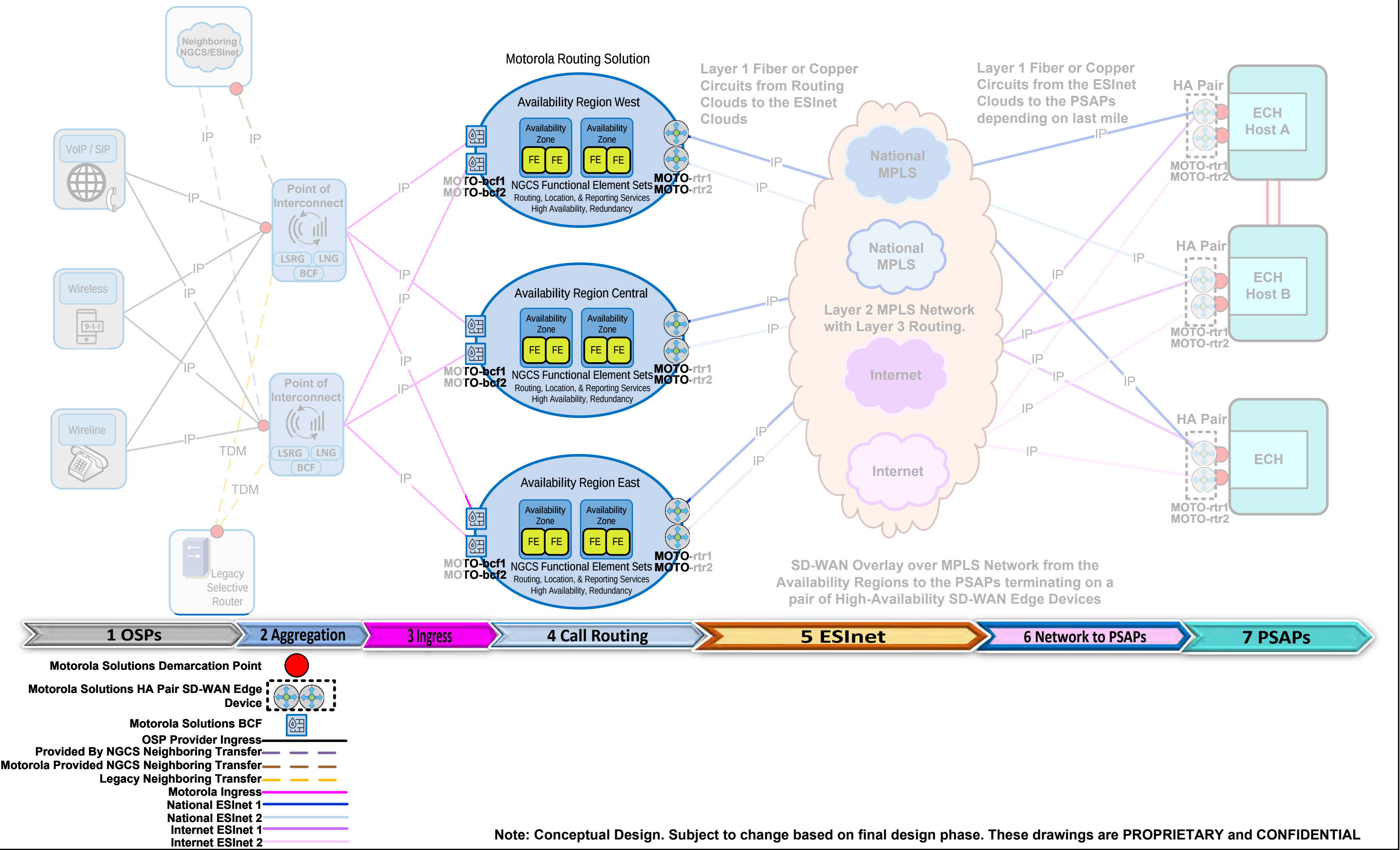
State of Nebraska – Solution Overview



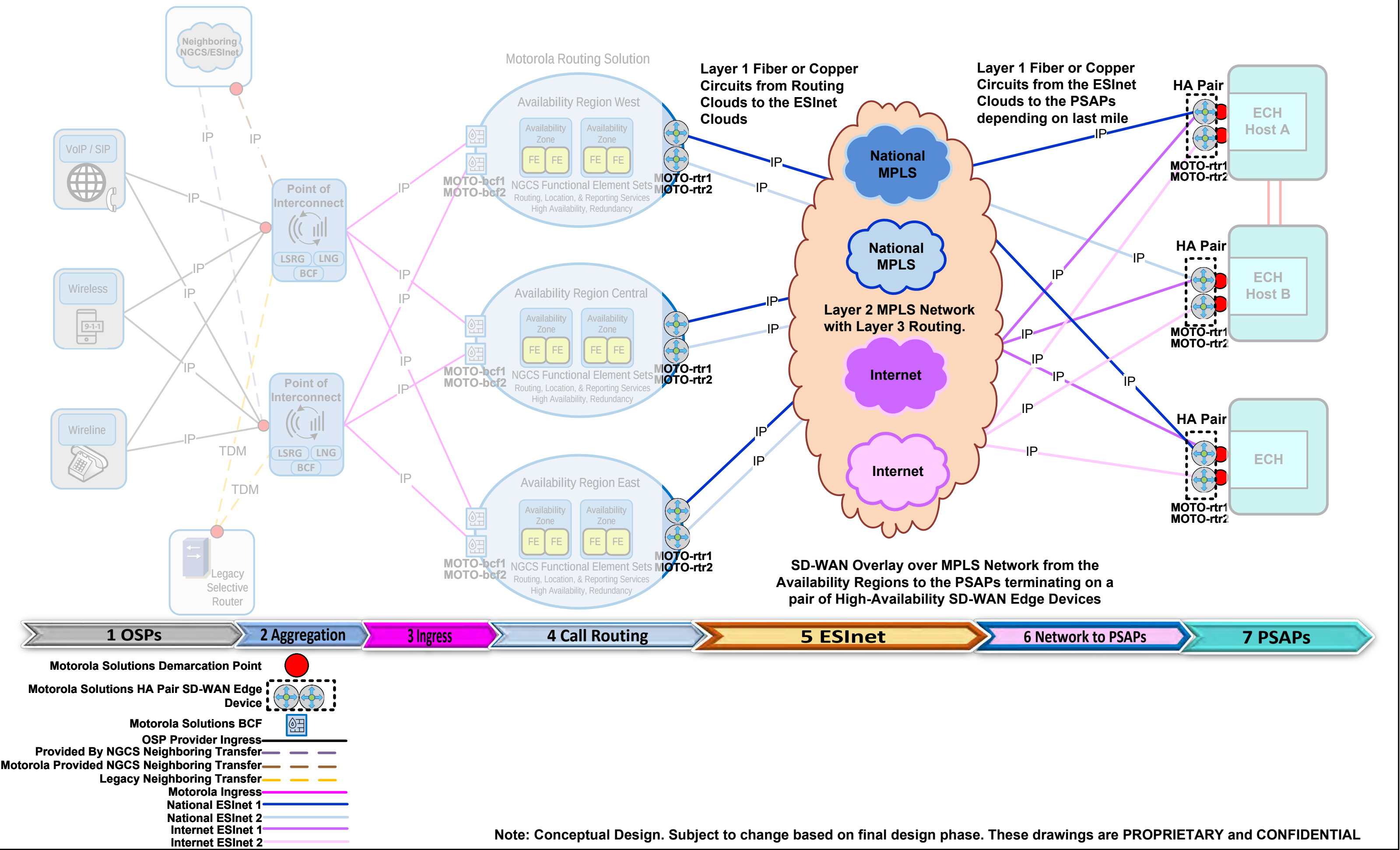
State of Nebraska – Solution Overview



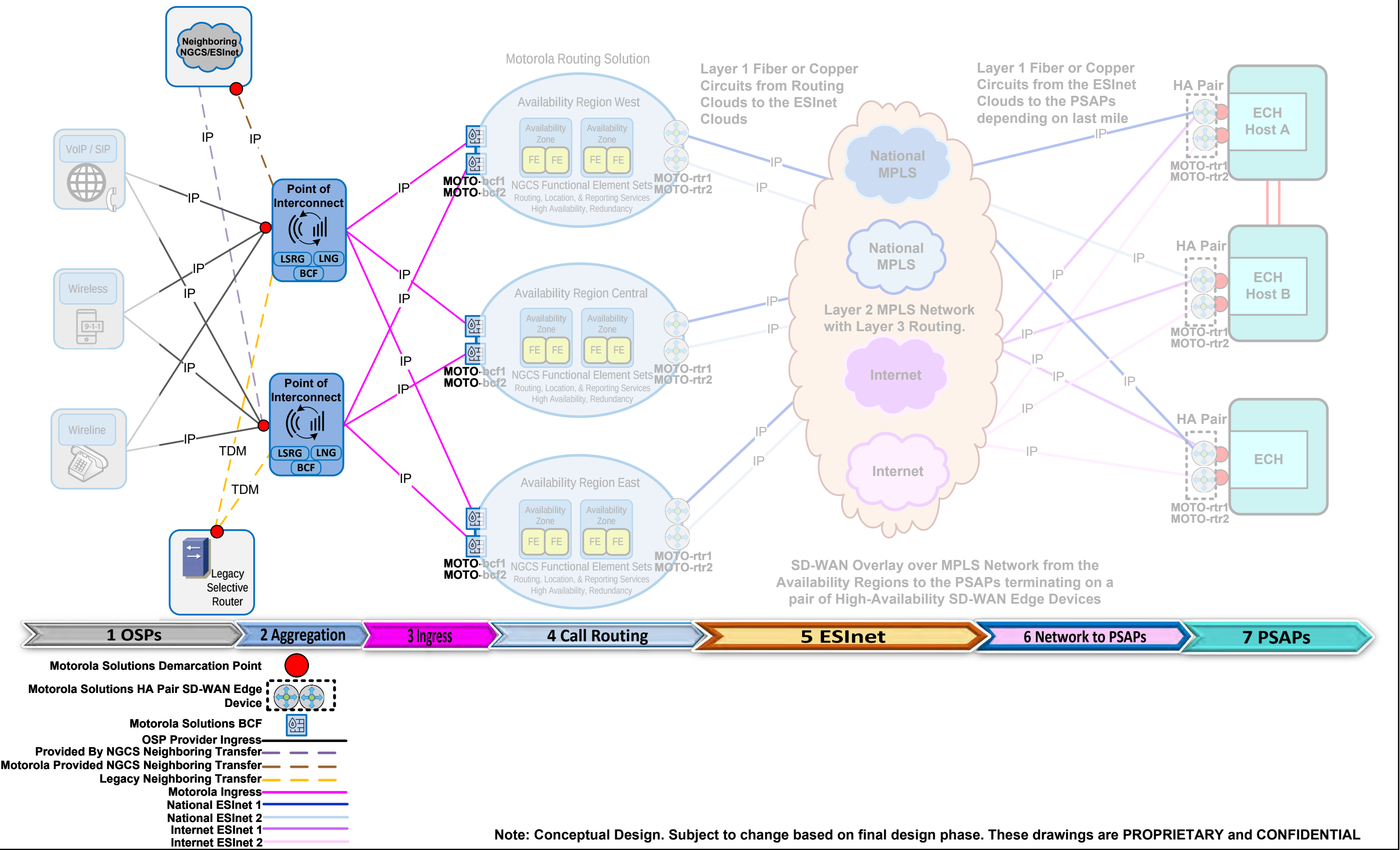
State of Nebraska – Solution Overview



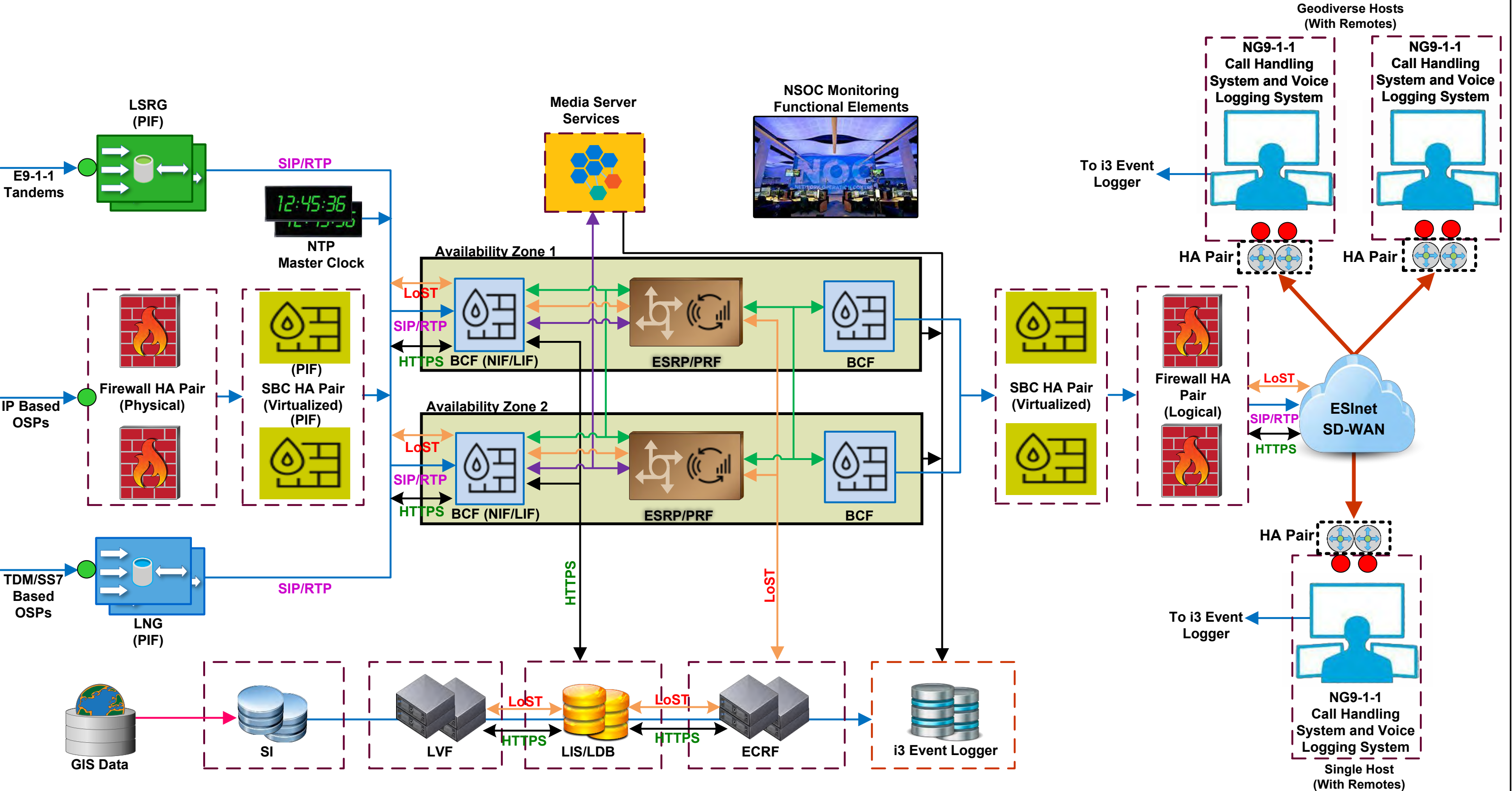
State of Nebraska – Solution Overview



State of Nebraska – Solution Overview



Functional Elements Diagram Per “Availability Region”



NOTE:
This drawing represents the redundant architecture of the Availability Zones within one Availability Region. There are 3 Availability Regions geographically separated for redundancy and resilience. All Availability Regions are identical in their design and structure and each can process 100% of the calls.

Legend:

- ESInet Demarcation Point
- Ingress Demarc
- ← 3 ESInet Circuits Per Site (1-MPLS 2-Broadband)

NGCS ESInet Circuits						MPLS	MPLS	Broadband 1	Broadband 1	Broadband 2	Broadband 2
Site #	Host Site Name	Address	City	State	ZIP	Access Capacity Quoted (Mbps)	Port Capacity Quoted (Mbps)	Download Speed Quoted (Mbps)	Upload Speed Quoted (Mbps)	Download Speed Quoted (Mbps)	Upload Speed Quoted (Mbps)
1	Boyd-Holt Counties Joint E911 - Host A	204 N. 4th St	O'NEILL	NE	68763	50	50	300	50	150	20
2	Cherry County - Host B	365 N MAIN ST Suite #9	VALENTINE	NE	69201	50	50	55	10	150	20
3	City of Columbus (Columbus-Platte Cty) - Host A	1304 BILL BABKA DR	COLUMBUS	NE	68601	10	10	500	20	300	300
4	City of Grand Island (Hall County) - Host B	1210 NORTH RD	GRAND ISLAND	NE	68803	10	10	500	20	500	20
5	City of Norfolk - Host A	202 N 7TH STREET	NORFOLK	NE	68701	10	10	500	20	25	30
6	City of South Sioux City (Dakota County) - Host B	701 W 29TH ST	SOUTH SIOUX CITY	NE	68776	10	10	500	20	150	30
7	Colfax County - Host A	411 E 11th St	Schuyler	NE	68661	10	5	300	30	300	30
8	Fremont Dodge Communications Center - Host B	725 N. Park Ave.	Fremont	NE	68025	10	5	500	20	300	300
9	DOUGLAS COUNTY COMMUNICATIONS - Single HostW/Remote	3603 N 156TH ST	OMAHA	NE	68116	10	5	100	20	25	15
10	Buffalo County Sheriff Office - Host A	2025 AVENUE A	KEARNEY	NE	68847	20	20	500	20	300	300
11	Dawson County - Host B	709 N GRANT	LEXINGTON	NE	68850	20	20	500	20	150	30

Exhibit 7 NIOC PCA Validation Policy

NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines

Abstract: This document 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.



NG9-1-1 Interoperability Oversight Commission (NIOC) Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Validation Guidelines

V1.0.0

NIOC Approval: 2/9/2022

Prepared at the request of NIOC by:
National Emergency Number Association (NENA) 9-1-1 Core Services Committee, PCA
Certificate Policy Working Group

Published by NIOC
Printed in USA



34 1 Background

35 This is a companion document to the NG9-1-1 Interoperability Oversight Commission (NIOC)
36 Certificate Policy (CP). This CP is available at <https://ng911ioc.org/library>.¹ The CP states:

37
38 *Certification Authorities (CAs), and the infrastructure they support, form the basis for*
39 *one of the primary mechanisms for providing assurance of identity. The widely placed*
40 *trust in CAs is at the heart of security mechanisms used to protect sessions and*
41 *transactions for Next Generation 9-1-1 (NG9-1-1). National Emergency Number*
42 *Association's (NENA's) i3 and associated standards require Transport Layer Security*
43 *(TLS) throughout the ecosystem to allow for secure communications and a single shared*
44 *root of trust to assist with interoperability. TLS relies on CAs to identify Servers and*
45 *Clients. The root of trust in the NG9-1-1 Public Key Infrastructure (PKI) is the Public*
46 *Safety Answering Point (PSAP) Credentialing Agency (PCA).*

47 *The purpose of this document is to provide security requirements needed to support the*
48 *secure issuance of Certificates in NG9-1-1 by the PCA CAs in the NG9-1-1 PKI. In*
49 *particular, this document has been developed to provide an appropriate level of*
50 *assurance to support government emergency services including public safety, and*
51 *applications, i.e., a high level of assurance as defined in the Validation Policy (VP). The*
52 *level of assurance refers to the strength of the Binding between the Public Key and the*
53 *entity whose name is cited in the Certificate, the policies used to control the use of the*
54 *corresponding Private Key, and the overall security provided by the PKI itself.*

55 *The PCA is a functional element in the NENA i3 Standard for Next Generation 9-1-1 core*
56 *services² which establishes a root of trust for the NG9-1-1 ecosystem to facilitate*
57 *interoperable security between disparate NG9-1-1 environments. The i3 standard*
58 *includes not only a shared root of trust to build a PKI, but it also standardizes how*
59 *identities are conveyed across NG9-1-1, and what roles those identities have in the*
60 *NG9-1-1 ecosystem. In addition to participating within a PKI in a trusted environment,*
61 *the standardization of conveying identities and roles provides for powerful abilities to*
62 *manage permissions and other security configurations in NG9-1-1 that work across*
63 *different NG9-1-1 environments and disparate public safety systems. The PCA as set*
64 *forth in this document supports all of the functionality as required by the i3 standard to*
65 *provide a PCA.³*

66 While the CP provides for guidance on certificate issuance, management and how the PKI
67 infrastructure is operated, the CP states throughout that validation procedures for Participants
68 will be handled in a separate Validation Policy.⁴ This document is that Validation Policy. It

¹ See NIOC Certificate Policy, available at <https://ng911ioc.org/library/>, last retrieved 5 May 2021 ("CP").

² See NENA STA-010.3-2021. Available at https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-010.3-2021_i3_stand.pdf. ("i3")

³ See CP at "Foreword".

⁴ See Id.



69 incorporates the whole of the CP by reference. As of this writing, that is version 1.01 of the CP
70 dated 03/10/2021.

71 **1.1 Governing Authority**

72 The governance structure that represents the participants for a PKI is known as the Policy
73 Authority (PA). The NG9-1-1 Interoperability Oversight Commission (NIOC) was convened by
74 the NENA Executive Board to serve as the independent PA for the PCA. The PA is responsible
75 for identifying the appropriate set of requirements for a given community and oversees the CAs
76 that issue Certificates for that community.
77

78 **1.2 Guidelines for the Issuance and Management of NG9-1-1 Certificates**

79 NIOC utilized the CA/Browser Forum's Guidelines for the Issuance and Management of
80 Extended Validation Certificates, also known as the Extended Validation Guidelines to create
81 this document (the "Guidelines"). Version 1.7.2 of the Extended Validation Guidelines served as
82 a baseline to establish the Guidelines for issuing NG9-1-1 certificates.⁵

83 These Guidelines describe an integrated set of technologies, protocols, identity proofing,
84 lifecycle management, and auditing practices specifying the minimum requirements that must
85 be met in order to issue and maintain NG9-1-1 Certificates. Subject information from valid
86 NG9-1-1 Certificates can then be used in a special manner by certain relying-party software
87 applications (e.g., Next Generation Core 9-1-1 Services [NGCS] applications) in order to provide
88 users with a trustworthy confirmation of the identity and/or Role of an entity in NG9-1-1.

89 In NG9-1-1, every entity carries a certificate. Validation for NG9-1-1 is done in a manner largely
90 in sync with prevailing guidelines for extended validation in operating commercial CA services,
91 but with specific and substantial changes that reflect unique circumstances in NG9-1-1.

92 The trust chain that comprises the NG9-1-1 PKI sits at the heart of security and interoperability
93 in NG9-1-1. Holding an NG9-1-1 Certificate affords an entity a substantial amount of privilege
94 within the NG9-1-1 environment, as NENA's i3 and related standards describe hundreds of
95 interactions that MUST be accepted so long as the interaction is initiated by an entity with an
96 NG9-1-1 certificate. A malicious entity holding an NG9-1-1 Certificate presents substantial risk
97 to the emergency calling infrastructure of the United States, Canada, Europe and beyond.
98 Accordingly, issuance of an NG9-1-1 certificate requires a very high level of scrutiny and
99 investigation prior to issuing a certificate.

100 As of this writing, these Guidelines assume a PKI that covers the NG9-1-1 systems of the United
101 States. These Guidelines also assume an objective to establish interoperability with the
102 emergency calling systems of Europe and Canada under the assumption that they will employ a

⁵ Version 1.7.2 represented the Extended Validation Guidelines, as adopted by the CA/Browser Forum as of Ballot SC27, passed by the Forum on 19 February 2020 and effective as of 27 March 2020. Copyright © 2007-2020, members of the CA/Browser Forum. This work is licensed under a Creative Commons Attribution 4.0 International license.



103 substantially similar trust framework. These Guidelines assume an update to this document will
104 be required in establishing such expansion or interoperability of the PKI beyond the United
105 States.

106 **1.3** Document History

Version	Description	Adopted	Effective
1.0.0	Initial NG9-1-1 Certificate Validation Guidelines development for NIOC	2/9/2022	2/9/2022

107

108



Table of Contents

111	1	BACKGROUND	2
112	1.1	GOVERNING AUTHORITY	3
113	1.2	GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF NG9-1-1 CERTIFICATES	3
114	1.3	DOCUMENT HISTORY	4
115	2	SCOPE	9
116	3	PURPOSE	9
117	3.1	PURPOSE OF NG9-1-1 CERTIFICATES	9
118	3.2	TYPES OF NG9-1-1 CERTIFICATES	9
119	3.3	PRIMARY PURPOSES	10
120	3.3.1	<i>Explicit Assurances</i>	10
121	3.3.2	<i>Identify Certification Authorities in the NG9-1-1 PKI</i>	11
122	3.3.3	<i>Identify and Describe the Role(s) of Agents in the NG9-1-1 PKI</i>	11
123	3.3.4	<i>Identify and Describe the Role(s) of Elements in the NG9-1-1 PKI</i>	11
124	3.3.5	<i>Identify and Describe Roles</i>	11
125	3.3.6	<i>Secure Transactions Inside of NG9-1-1 Through Explicit Trust</i>	11
126	3.3.7	<i>Signing of Records</i>	12
127	3.4	SECONDARY PURPOSES	12
128	3.4.1	<i>Secure Transactions Into/Outside of the NG9-1-1 PKI Through Explicit Trust</i>	12
129	3.5	EXCLUDED PURPOSES	12
130	3.6	DOCUMENTS INCORPORATED BY REFERENCE AND REFERENCES	12
131	3.7	DEFINITIONS	12
132	3.8	ABBREVIATIONS AND ACRONYMS	17
133	3.9	CONVENTIONS	17
134	4	CERTIFICATE WARRANTIES AND REPRESENTATIONS	18
135	4.1	NG9-1-1 CERTIFICATE WARRANTIES	18
136	4.2	BY THE APPLICANT	19
137	5	COMMUNITY AND APPLICABILITY	19
138	5.1	ISSUANCE OF NG9-1-1 CERTIFICATES	19
139	5.2	NG9-1-1 POLICIES	19
140	5.2.1	<i>Implementation</i>	19
141	5.2.2	<i>Disclosure</i>	19
142	5.3	COMMITMENT TO COMPLY WITH RECOMMENDATIONS	19
143	5.4	INSURANCE	20
144	5.5	OBTAINING NG9-1-1 CERTIFICATES	20
145	5.5.1	<i>General</i>	20
146	5.5.2	<i>Private Entity Subjects</i>	20
147	5.5.3	<i>Public Safety Entity Subjects</i>	20
148	5.5.4	<i>Business Entity Subjects</i>	21
149	5.5.5	<i>Non-Commercial Entity Subjects</i>	21
150	6	NG9-1-1 CERTIFICATE CONTENT AND PROFILE	22
151	6.1	ISSUER INFORMATION	22

152	6.2	SUBJECT DISTINGUISHED NAME FIELDS	22
153	6.3	SUBJECT COMMON NAME FIELD	22
154	6.4	SUBJECT JURISDICTION OF INCORPORATION OR REGISTRATION FIELD	22
155	6.4.1	<i>Subject Registration Number Field</i>	22
156	6.4.2	<i>Subject Organizational Unit Name Field</i>	22
157	6.5	SUBJECT ORGANIZATION IDENTIFIER FIELD	22
158	6.6	OTHER SUBJECT ATTRIBUTES	22
159	6.7	CERTIFICATE POLICY IDENTIFICATION	22
160	6.8	CERTIFICATE POLICY IDENTIFICATION REQUIREMENTS	22
161	6.9	SUBSCRIBER CERTIFICATES	22
162	6.10	ROOT CA CERTIFICATES	22
163	6.11	SUBORDINATE ICA CERTIFICATES	23
164	6.12	SUBSCRIBER CERTIFICATES	23
165	6.13	MAXIMUM VALIDITY PERIOD FOR CERTIFICATES	23
166	6.14	SUBSCRIBER PUBLIC KEY	23
167	6.15	CERTIFICATE SERIAL NUMBER	23
168	6.16	ADDITIONAL TECHNICAL REQUIREMENTS FOR VALIDATING CERTIFICATES	23
169	6.17	CERTIFICATE EXTENSIONS	23
170	6.17.1	<i>Subject Alternative Name Extension</i>	23
171	6.17.2	<i>Organization Identifier Field</i>	23
172	7	NG9-1-1 CERTIFICATE REQUEST REQUIREMENTS	23
173	7.1	GENERAL REQUIREMENTS	23
174	7.2	DOCUMENTATION REQUIREMENTS	23
175	7.3	ROLE REQUIREMENTS	24
176	7.4	REQUIREMENTS FOR SUBSCRIBER AGREEMENT AND TERMS OF USE	24
177	7.5	NG9-1-1 CERTIFICATE REQUEST REQUIREMENTS	24
178	8	VERIFICATION REQUIREMENTS	25
179	8.1	GENERAL OVERVIEW	25
180	8.2	VERIFICATION REQUIREMENTS FOR NG9-1-1 CERTIFICATE TYPES	25
181	8.2.1	<i>Verification of the Root Certificate</i>	25
182	8.2.2	<i>Verification of ICA Certificates</i>	25
183	8.2.3	<i>Verification of Agency Certificates</i>	25
184	8.2.4	<i>Verification of all Other Certificates</i>	25
185	8.3	VERIFICATION METHODS	25
186	8.3.1	<i>Acceptable Methods of Verification – Overview</i>	25
187	8.4	VERIFICATION OF ROLE	25
188	8.5	VERIFICATION OF AGENCY IDENTITY	26
189	8.5.1	<i>DNS Change</i>	26
190	8.5.2	<i>IP Address</i>	26
191	8.5.3	<i>Any Other Method</i>	28
192	8.6	VERIFICATION OF OWNER	29
193	8.6.1	<i>Verification of Owner for Agency Certificates</i>	29
194	8.7	VERIFICATION OF APPLICANT'S LEGAL EXISTENCE AND IDENTITY	29
195	8.7.1	<i>Verification Requirements</i>	29
196	8.7.2	<i>Acceptable Method of Verification</i>	30
197	8.8	VERIFICATION OF APPLICANT'S PHYSICAL EXISTENCE – PLACE OF OPERATIONS	31
198	8.8.1	<i>Verification Requirements</i>	31
199	8.8.2	<i>Acceptable Methods of Verification</i>	31
200	8.9	VERIFIED METHOD OF COMMUNICATION	32

201	8.9.1	Verification Requirements	32
202	8.9.2	Acceptable Methods of Verification	32
203	8.9.3	Verification of Applicant's Operational Existence	32
204	8.9.4	Verification Requirements	32
205	8.10	VERIFICATION OF NAME, TITLE, AND AUTHORITY OF CONTRACT SIGNER AND CERTIFICATE APPROVER	33
206	8.10.1	Verification Requirements	33
207	8.10.2	Acceptable Methods of Verification – Name, Title and Legal Agency.....	33
208	8.10.3	Acceptable Methods of Verification – Signing Authority	34
209	8.10.4	Pre-Authorized Certificate Approver	36
210	8.11	VERIFICATION OF SIGNATURE ON SUBSCRIBER AGREEMENT AND NG9-1-1 CERTIFICATE REQUESTS.....	36
211	8.11.1	Verification Requirements	37
212	8.11.2	Acceptable Methods of Signature Verification	37
213	8.12	VERIFICATION OF APPROVAL OF NG9-1-1 CERTIFICATE REQUEST	37
214	8.12.1	Verification Requirements	37
215	8.12.2	Acceptable Methods of Verification	37
216	8.12.3	Independent Confirmation from Applicant.....	38
217	8.12.4	Qualified Independent Information Source (QIIS)	39
218	8.12.5	Qualified Government Information Source (QGIS)	40
219	8.12.6	Qualified Government Tax Information Source (QTIS)	40
220	8.13	OTHER VERIFICATION REQUIREMENTS.....	40
221	8.13.1	High Risk Status.....	40
222	8.13.2	Denied Lists and Other Legal Unapproved Lists	40
223	8.13.3	Parent/Subsidiary/Affiliate Relationship	41
224	8.14	FINAL CROSS-CORRELATION AND DUE DILIGENCE	41
225	8.15	REQUIREMENTS FOR RE-USE OF EXISTING DOCUMENTATION	42
226	8.15.1	Validation For Existing Subscribers	42
227	8.15.2	Re-issuance Requests.....	42
228	8.15.3	Age of Validated Data.....	43
229	9	CERTIFICATE ISSUANCE BY A ROOT CA	43
230	9.1.1	Identity and Background Verification	43
231	10	CERTIFICATE REVOCATION AND STATUS CHECKING	44
232	11	EMPLOYEE AND THIRD PARTY ISSUES	44
233	11.1	TRUSTWORTHINESS AND COMPETENCE	44
234	11.1.1	Training and Skills Level	44
235	11.1.2	Separation of Duties.....	44
236	11.2	DELEGATION OF FUNCTIONS TO REGISTRATION AUTHORITIES AND SUBCONTRACTORS	44
237	11.2.1	General	44
238	11.2.2	Local Registration Authority (LRA).....	44
239	11.2.3	Guidelines Compliance Obligation.....	45
240	11.2.4	Allocation of Liability	45
241	12	DATA RECORDS	45
242	13	DATA SECURITY	45
243	14	AUDIT	45
244	14.1	ELIGIBLE AUDIT SCHEMES	45
245	14.2	PER THE CP AUDIT PERIOD.....	45
246	14.3	AUDIT RECORD	46
247	14.4	PRE-ISSUANCE READINESS AUDIT	46

248	14.5	PER THE CP REGULAR SELF AUDITS	46
249	14.6	PER THE CP AUDITOR QUALIFICATION	46
250	14.7	PER THE CP ROOT CA KEY PAIR GENERATION	46
251	15	LIABILITY AND INDEMNIFICATION	46
252	16	ACKNOWLEDGEMENTS.....	46
253			
254			

255 **2 Scope**

256 These Guidelines for the issuance and management of NG9-1-1 Certificates describe certain of
257 the minimum requirements that a CA must meet in order to issue Certificates for NG9-1-1 in
258 accordance with NENA standards and in accordance with policies and procedures established by
259 NIOC to establish a PKI for NG9-1-1. These Guidelines incorporate the requirements established
260 by the NIOC CP by reference.

261 Entities can be CAs, Agencies, Users, Elements or Devices. Each of these entities is validated
262 prior to issuance of a certificate in accordance with these Guidelines. The Root Certificate for
263 the NG9-1-1 PKI is the PSAP Credentialing Agency (PCA), which is operated by NIOC.

264 **3 Purpose**

265 **3.1 Purpose of NG9-1-1 Certificates**

266 NG9-1-1 Certificates are intended to:

- 267 • sign certificates of subsidiary Intermediate Certification Authorities (ICAs)
268 • provide for interoperability in NG9-1-1 through explicit trust
269 • provide for security through establishing TLS within a PKI
270 • verify the authenticity of signed Records
271 • provide non-repudiation of signed Records
272 • express an entity identity and Role within the trust chain for NG9-1-1
273 • verify the authenticity of executable code in NG9-1-1.

274 NG9-1-1 Certificates MUST be used for some of these actions, and MAY be used for others
275 as described in these Guidelines.

276 **3.2 Types of NG9-1-1 Certificates**

277 NG9-1-1 Certificates fall into multiple categories and are either CA Certificates credentialing a
278 CA or an end-entity Certificate credentialing an Agency, Service, User, Element, or Role. Below
279 is a summary of the types of NG9-1-1 Certificates allowable under these Guidelines.
280

Type of Cert	Description	Validation Done By
Root Certificate	The offline root certificate comprising the basis of the trust chain for the PKI.	Self-signed by the root CA in an auditable ceremony per the CP.
ICA Certificate	A certificate for an ICA.	The RA for the CP for a Tier-2 ICA, or the RA in the CPS governing the signing ICA.
Agency Certificate	A certificate issued to an agency. ID example: psap.fairfax.virginia.us	The RA for the ICA.



Type of Cert	Description	Validation Done By
Service Certificate	A certificate issued to a service instance in a particular NGCS or Agency	The RA or LRA for a CA with Delegated Authority to perform Validation
Element Certificate	A certificate issued to a physical or virtual entity that is addressable and has a unique identity (elementID)	The RA or LRA for a CA with Delegated Authority to perform Validation.
User Certificate (Agent)	A certificate issued to a person or automaton*. These are always issued by an ICA. ID example: dhandy@psap.fairfax.virginia.us	The RA or LRA for a CA with Delegated Authority to perform Validation.

*future work

3.3 Primary Purposes

The primary purposes of NG9-1-1 Certificates are described in the following subsections.

3.3.1 Explicit Assurances

NG9-1-1 Certificates focus on the identity of the Identifier⁶ in the SubjectAltName in the Certificate as well as the behavior of the Identity within the NG9-1-1 PKI and chain of trust for NG9-1-1. As such, contrary to Certificates used for commercial purposes, an NG9-1-1 Certificate SHALL provide explicit assurances as to the following:

1. That the Identity named in the NG9-1-1 Certificate is a legitimate and trustworthy NG9-1-1 entity;
2. That the Identity named in the NG9-1-1 Certificate complies with applicable laws;
3. That it is "safe" to conduct NG9-1-1 operations with the Identity named in the NG9-1-1 Certificate.

The NG9-1-1 PKI policy requirements support the secure issuance of Certificates in NG9-1-1 by the PCA CAs. These policies reflect a High level of Assurance commensurate with NIST SP-800-63 series Identity Assurance Level 3.⁷ A table outlining NIST Assurance levels is below:

⁶ "Identifier" has the meaning as specified in i3 at Section 2.1.

⁷ See NIST 800-63 at Section 6, Retrieved 2 November 2020 at: <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec6>.



Impact Categories	Assurance Level		
	1	2	3
Inconvenience, distress or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	N/A	Low/Moderate	High
Unauthorized release of sensitive information	N/A	Low/Moderate	High
Personal Safety	N/A	Low	Moderate/High
Civil or criminal violations	N/A	Low/Moderate	High

297

298 3.3.2 Identify Certification Authorities in the NG9-1-1 PKI

299 The NG9-1-1 PKI includes two types of CAs: the Root Certification Authority, which is the PCA,
300 and ICAs, which are either signed by the Root Certificate or are signed by an ICA in accordance
301 with the CP.

302 3.3.3 Identify and Describe the Role(s) of Agents in the NG9-1-1 PKI

303 The NG9-1-1 PKI includes a population of Agents. Public safety personnel, the devices they use
304 and/or devices that take actions throughout the PKI comprise this population of Agents. Agent
305 Certificates include the identity of the Agent, their Agency affiliation and a list of their Roles in
306 the NG9-1-1 PKI.

307 3.3.4 Identify and Describe the Role(s) of Elements in the NG9-1-1 PKI

308 The NG9-1-1 PKI includes a population of Elements and Services. Element or Service
309 Certificates credential either Functional Elements or Services within the NG9-1-1 PKI as
310 described in i3. An Element Certificate will include the identity of the Element, its Agency
311 affiliation, and a list of its Role(s) in the NG9-1-1 PKI.

312 3.3.5 Identify and Describe Roles

313 Agents, Elements, Services and CAs hold one or more Roles in the NG9-1-1 PKI. These Roles
314 are used to express what the Element or Agent is allowed to do within the PKI. When
315 performing Validation, the Validator SHALL validate that the Applicant has a legitimate and valid
316 purpose to act in one or more Roles within the NG9-1-1 PKI using the process as described
317 below.

318 3.3.6 Secure Transactions Inside of NG9-1-1 Through Explicit Trust

319 Transactions in NG9-1-1 are allowed provided that the initiator presents credentials traceable to
320 the PCA. By establishing a PKI with a shared root of trust, the NG9-1-1 community can safely
321 and securely engage in transactions within and between different NG9-1-1 systems and can
322 achieve interoperability by having a shared convention for establishing trustworthiness of
323 entities between different systems as well as what Roles entities are allowed to perform
324 between these systems.



325 3.3.7 Signing of Records
326 NG9-1-1 allows for the signing of Records, including records in a public safety communications
327 logger or JSON payloads signed with JWS. When signing is required, records are signed with a
328 Certificate traceable to the PCA.⁸

329 **3.4 Secondary Purposes**

330 Secondary purposes of NG9-1-1 are described in the following subsections.

331 3.4.1 Secure Transactions Into/Outside of the NG9-1-1 PKI Through Explicit Trust

332 It is a long-term objective to establish or investigate feasibility of establishing shared trust
333 between the NG9-1-1 PKI and other PKIs for interoperability purposes, including the Federal
334 Bridge Certification Authority, PKI(s) that may be established for any Public Safety Broadband
335 Networks, the SHAKEN CA and/or PKIs established for next-generation emergency calling
336 environments internationally that Relying Parties in the NG9-1-1 PKI have reason and need to
337 interoperate with. Accordingly, it is a secondary purpose of NG9-1-1 Certificates to secure
338 transactions and establish interoperability with other trust environments once trust is
339 established between the PCA and any other Root CA.

340 **3.5 Excluded Purposes**

341 NG9-1-1 Certificates are not intended to be used outside of public safety for identity proofing
342 for commercial or general identity proofing purposes, such as to secure access to a public
343 website through TLS, electronically signing emails or documents unless as expressly required
344 for interoperable NG9-1-1 communications or signing executable code for commercial
345 applications unless used for NG9-1-1 or public safety operations.

346 **3.6 Documents Incorporated by Reference and References**

- 347 • NENA STA-010.2-2016, incorporated by reference
- 348 • NENA STA-010.3-2021, incorporated by reference
- 349 • NIOC CP v. 1.01 (Public Safety Answering Point (PSAP) Credentialing Agency (PCA)
350 Certificate Policy), incorporated by reference
- 351 • CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-
352 Trusted Certificates (v 1.6.4 and up) ("Baseline Requirements"), for reference only
- 353 • CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation
354 Certificates Guidelines v 1.7.2⁹

355 **3.7 Definitions**

356 Capitalized terms are defined in the Baseline Requirements and the CP except where provided
357 below:

⁸ See i3 at 5.10.

⁹ Retrieved 22 June 2021 at <https://cabforum.org/baseline-requirements-documents>. "Baseline Requirements"



358 Applicant: The entity or entities applying for a Certificate for a Subject.

359 Appropriate Authority: The governing body (whether governmental or otherwise) with legal
360 or other official responsibility to certify the legitimacy of certain claims regarding a Subject or
361 Applicant, such as the existence of a Public Safety Entity or Private Entity with a valid public
362 safety purpose or specific information about a Subject or Applicant. An Appropriate Authority
363 may maintain a Qualified Independent Information Source (QIIS) or Qualified Government
364 Information Source (QGIS), in which case the QIIS or QGIS is sufficient to validate information
365 and direct communication with the Appropriate Authority is not necessary.

366 Authority: A source other than the Certificate Approver, through which verification occurs that
367 the Certificate Approver is expressly authorized by the Applicant, as of the date of the NG9-1-1
368 Certificate Request, to take the Request actions described in these Guidelines.

369 Authorization Domain Name: A domain name used for the purposes of Validation under
370 these Guidelines.

371 Baseline Requirements: The Baseline Requirements for the Issuance and Management of
372 Publicly-Trusted Certificates as published by the CA/Browser Forum and any amendments to
373 such document.

374 Business Entity: This entity has the same meaning as "Private Entity".

375 Certificate Approver: A natural person who is either the Applicant, employed by the Applicant,
376 or an authorized agent who has express authority to represent the Applicant to (i) act as a
377 Certificate Requester and to authorize other employees or third parties to act as a Certificate
378 Requester, and (ii) to approve NG9-1-1 Certificate Requests submitted by other Certificate
379 Requesters.

380 Certificate Requester: A natural person who is either the Applicant, employed by the
381 Applicant, an authorized agent who has express authority to represent the Applicant, or a third
382 party that completes and submits an NG9-1-1 Certificate Request on behalf of the Applicant.

383 Confirmation Request: An appropriate out-of-band communication requesting verification or
384 confirmation of the particular fact at issue.

385 Confirming Person: A position within an Applicant's organization that confirms the particular
386 fact at issue.

387 Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or
388 an authorized agent who has express authority to represent the Applicant, and who has
389 authority on behalf of the Applicant to sign Subscriber Agreements.

390 Delegated Authority: The authorization to act on behalf of another entity for official
391 purposes, such as to act under contract to a Public Safety Entity as a Certificate Requester for
392 that Public Safety Entity, or to act as an RA or LRA.

393 Guidelines: This document.



394 NG9-1-1 Certificate: A certificate that contains subject information specified in these
395 Guidelines and that has been validated in accordance with these Guidelines.

396 NG9-1-1 Certificate Renewal: The process whereby an Applicant who has a valid unexpired
397 and non-Revoked NG9-1-1 Certificate makes an application, to the CA that issued the original
398 certificate, for a newly issued NG9-1-1 Certificate for the same organizational name and Domain
399 Name prior to the expiration of the Applicant's existing NG9-1-1 Certificate but with a new 'valid
400 to' date beyond the expiry of the current NG9-1-1 Certificate and a new serial number.

401 NG9-1-1 Certificate Reissuance: The process whereby an Applicant who has a valid
402 unexpired and non-revoked NG9-1-1 Certificate makes an application, to the CA that issued the
403 original certificate, for a newly issued NG9-1-1 Certificate for the same organizational name and
404 Domain Name prior to the expiration of the Applicant's existing NG9-1-1 Certificate but with a
405 'valid to' date that matches that of the current NG9-1-1 Certificate.

406 NG9-1-1 Certificate Request: A request from an Applicant to the CA requesting that the CA
407 issue an NG9-1-1 Certificate to the Applicant, which request is validly authorized by the
408 Applicant and signed by the Appropriate Authority.

409 NG9-1-1 Certificate Warranties: In conjunction with the CA issuing an NG9-1-1 Certificate,
410 the CA and its Root CA, during the period when the NG9-1-1 Certificate is Valid, promise that
411 the CA has followed the requirements of these Guidelines and the CA's NG9-1-1 Policies in
412 issuing the NG9-1-1 Certificate and in verifying the accuracy of the information contained in the
413 NG9-1-1 Certificate.

414 NG9-1-1 OID: An identifying number, in the form of an "object identifier," that is included in
415 the *certificatePolicies* field of a certificate that: (i) indicates which CA policy statement relates to
416 that certificate, and (ii) is either the PCA policy identifier or a policy identifier that, by pre-
417 agreement, marks the certificate as being an NG9-1-1 Certificate. The OID for this document is
418 maintained in a registry in accordance with the rules of the CP.

419 NG9-1-1 Policies: Auditable NG9-1-1 Certificate practices, policies and procedures, such as a
420 certification practice statement and certificate policy, that are developed, implemented, and
421 enforced by the Root CA and its subordinate CAs.

422 Incorporating Agency: In the context of a Private Entity, the government agency in the
423 Jurisdiction of Incorporation under whose authority the legal existence of the entity is
424 registered (e.g., the government agency that issues certificates of formation or incorporation).
425 In the context of a Public Safety Entity, the entity that enacts law, regulations, or decrees
426 establishing the legal existence of Public Safety Entities.

427 Independent Confirmation From Applicant: Confirmation of a particular fact received by
428 the CA pursuant to the provisions of the Guidelines or binding upon the Applicant.

429 Individual: A natural person.

430 Jurisdiction of Incorporation: In the context of a Private Organization, the country and
431 (where applicable) the state or province or locality where the organization's legal existence was

432 established by a filing with (or an act of) an appropriate government agency or entity (e.g.,
433 where it was incorporated). In the context of a Public Safety Entity, the country and (where
434 applicable) the state or province where the Entity's legal existence was created by law.

435 Jurisdiction of Registration: In the case of a Business Entity, the state, province, or locality
436 where the organization has registered its business presence by means of filings by a Principal
437 Individual involved in the business.

438 Legal Agency: Where an agent acts on behalf of a principal within the scope of their authority
439 which has been granted to them expressly or can be implied from the circumstances. Their acts
440 bind the principal and the third party unless it follows from the circumstances of the case that
441 the agent undertakes to bind themselves only.¹⁰

442 Legal Agent: An individual who has Legal Agency conferred upon them.

443 Legal Entity: A Private Entity, Public Safety Entity, or Non-Commercial Entity.

444 Legal Existence: A Private Entity, Public Safety Entity, or Business Entity has Legal Existence
445 if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

446 Local Registration Authority (LRA): A trusted party who may perform Validation and assert
447 the accuracy of information presented by the Certificate Requester and/or to the Certificate
448 Approver and/or on behalf of the RA. For example, supervisory personnel at a Public Safety
449 Entity may be deemed a Local Registration Authority to validate employees at their organization
450 to receive NG9-1-1 Certificates. See Section 11.2.2.

451 Place of Operation: The location of any entity (such as a PSAP, communications center or
452 headquarters) where the Applicant's operations are conducted.

453 Principal Individual: An individual of a Private Entity or Public Safety Entity, that is either an
454 owner, partner, managing member, director, or officer, as identified by their title of
455 employment, or an employee, contractor or Legal Agent authorized by such entity or
456 organization to conduct business related to the request, issuance, and use of NG9-1-1
457 Certificates.

458 Private Organization: A non-governmental legal entity (whether ownership interests are
459 privately held or publicly traded) whose existence was created by a filing with (or an act of) the
460 Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

461 Public Safety Entity: An entity officially charged with the safety of life and property, usually a
462 government organization, that may hold an NG9-1-1 Certificate in accordance with these
463 Guidelines.

464 Private Entity: An entity that is not a government organization that may hold an NG9-1-1
465 Certificate in accordance with these Guidelines in support of one or more Public Safety Entities.

¹⁰ Adapted from trans-lex.org legal dictionary. Retrieved 22 June 2021 from https://www.trans-lex.org/911000/_prerequisites-and-effects-of-agency/. This document does not provide legal advice.

466 Qualified Government Information Source (QGIS): A database maintained by a
467 government organization (e.g. SEC filings) that meets the requirements of these Guidelines.

468 Qualified Government Tax Information Source (QTIS): A Qualified Governmental
469 Information Source that specifically contains tax information relating to Private Organizations,
470 Business Entities, or Individuals.

471 Qualified Independent Information Source (QIIS): A regularly-updated and current,
472 publicly available, database designed for the purpose of accurately providing the information for
473 which it is consulted, and which is generally recognized as a dependable source of such
474 information.

475 Registration Agency: A Governmental Agency that registers business information in
476 connection with an entity's business formation or authorization to conduct business under a
477 license, charter or other certification. A Registration Agency MAY include but is not limited to (i)
478 a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a
479 State Department of Insurance; or (iii) a chartering agency, such as a state office or department
480 of financial regulation, banking or finance, or a federal agency such as the Office of the
481 Comptroller of the Currency or Office of Thrift Supervision.

482 Registered Agent: An individual or entity that is: (i) authorized by the Applicant to receive
483 service of process and business communications on behalf of the Applicant; and (ii) listed in the
484 official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in
485 (i) above.

486 Registration Authority (RA): Per the CP.

487 Registration Number: The unique number assigned to a Private Organization by the
488 Incorporating Agency in such entity's Jurisdiction of Incorporation.

489 Role: An enumerated role in the NG9-1-1 PKI maintained in a registry. One or more Roles may
490 be assigned to any NG9-1-1 PKI member.

491 Signing Authority: One or more Certificate Approvers designated to act on behalf of the
492 Applicant.

493 Sponsorship: The act of a Public Safety Entity taking responsibility for a Private Entity's
494 possession of an NG9-1-1 Certificate.

495 Subject: Per the CP.

496 Validation: The act of validating an entity to be a part of the NG9-1-1 PKI in accordance with
497 this policy, which includes verifying the identity of the entity requesting a Certificate, confirming
498 their Agency affiliation, and validating that the requester has a legitimate and valid purpose to
499 participate in the NG9-1-1 PKI.

3.8 Abbreviations and Acronyms

Term	Expansion
BIS	(US Government) Bureau of Industry and Security
CSO	Chief Security Officer
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
NENA	NENA: The 9-1-1 Association (or National Emergency Number Association)
NG9-1-1	Next-Generation 9-1-1
NGCS	Next Generation Core Services
NIOC	NG9-1-1 Interoperability Oversight Commission
PCA	PSAP Credential Agency
PSAP	Public Safety Answering Point
IRS	Internal Revenue Service
ISP	Internet Service Provider
QGIS	Qualified Government Information Source
QTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
SEC	(US Government) Securities and Exchange Commission

501

3.9 Conventions

503 Terms not otherwise defined in these Guidelines shall be as defined in applicable agreements,
504 user manuals, Certification Practice Statements (CPSes), and Certificate Policies (CP) of the CA
505 issuing NG9-1-1 Certificates.

506 This section defines keywords, as they are be interpreted in NENA documents. The form of
507 emphasis (UPPER CASE) shall be consistent and exclusive throughout the document. Any of
508 these words used in lower case and not emphasized do not have special significance beyond
509 normal usage.

- 510 1. MUST, SHALL, REQUIRED: These terms mean that the definition is a normative (absolute)
511 requirement of the specification.
- 512 2. MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an
513 absolute prohibition of the specification.



3. SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option "must" be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option "must" be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

These definitions are based on IETF RFC 2119.¹¹

4 Certificate Warranties and Representations

4.1 NG9-1-1 Certificate Warranties

When the CA issues an NG9-1-1 Certificate, the CA represents and warrants to Relying Parties, during the period when the NG9-1-1 Certificate is Valid, that the CA, or the RA or LRA on the CA's behalf, has followed the requirements of these Guidelines and the Certificate Policy and applicable CPS in issuing and managing the NG9-1-1 Certificate and in verifying the accuracy of the information contained in the NG9-1-1 Certificate. The NG9-1-1 Certificate Warranties specifically include, but are not limited to, the following:

1. Legal Existence: The CA or RA or LRA has confirmed with the Appropriate Authority in the Subject's Jurisdiction of Incorporation that, as of the date the NG9-1-1 Certificate was issued, the Subject named in the NG9-1-1 Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation;
2. Identity: The CA or RA or LRA has confirmed that, as of the date the NG9-1-1 Certificate was issued, that the Identifier, Role(s), Agency affiliation, and Owner are correct and have been validated by an RA or LRA in the NG9-1-1 validation chain.
3. Accuracy of Information: The CA has taken all steps reasonably necessary to verify that all of the other information in the NG9-1-1 Certificate is accurate, as of the date the NG9-1-1 Certificate was issued;

¹¹ <https://datatracker.ietf.org/doc/html/rfc2119>

4. Subscriber Agreement: The Subject named in the NG9-1-1 Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA or RA or LRA that satisfies the requirements of these Guidelines or, if they are affiliated, the Agency has acknowledged and accepted the Terms of Use;
5. Status: The CA will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the NG9-1-1 Certificate as Valid or Revoked, and consistent with the CP and the applicable CPS; and
6. Revocation: The CA or RA or LRA will follow the requirements of these Guidelines and revoke the NG9-1-1 Certificate for any of the revocation reasons specified in these Guidelines, and consistent with the CP and the applicable CPS.

4.2 By the Applicant

NG9-1-1 Certificate Applicants make the commitments and warranties set forth in the NG9-1-1 CP and the applicable CPS.

5 Community and Applicability

5.1 Issuance of NG9-1-1 Certificates

The CA MAY issue NG9-1-1 Certificates, provided that the Root CA and its subordinate CAs satisfy the requirements in these Guidelines and the applicable CP and CPS.

If a court or government body with jurisdiction over the activities covered by these Guidelines determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify NIOC of the facts, circumstances, and law(s) involved, so that NIOC may revise these Guidelines accordingly.

5.2 NG9-1-1 Policies

5.2.1 Implementation

Each CA and Relying Party SHALL conform with all requirements in NENA i3 Standard and the NIOC CP and the applicable CPS.

5.2.2 Disclosure

Per the CP.

5.3 Commitment to Comply with Recommendations

Each CA SHALL publicly give effect to these Guidelines and represent that they will adhere to the latest published version by incorporating them into their respective CPSes, using a clause such as the following (which must include a link to the official version of these Guidelines):



[Name of CA] conforms to the current version of the NG9-1-1 Interoperability Oversight Commission Certificate Policy and Validation Policy published at ng911ioc.org. In the event of any inconsistency between this document and those policies, those policies take precedence over this document.

A valid link SHALL always be maintained by NIOC, subject to best-effort availability, at:
<https://ng911ioc.org/library>

In addition, the CA MUST include (directly or by reference) the applicable requirements of these Guidelines in all contracts with Subordinate CAs, RAs, LRAs, and subcontractors that involve or relate to the issuance or maintenance of NG9-1-1 Certificates. The CA MUST enforce compliance with such terms.

5.4 Insurance

No stipulation.

5.5 Obtaining NG9-1-1 Certificates

5.5.1 General

The CA MAY only issue NG9-1-1 Certificates to Applicants that meet the Private Entity, Public Safety Entity and Non-Commercial Entity requirements specified below.

5.5.2 Private Entity Subjects

Private Entities are eligible to be issued NG9-1-1 Certificates in the capacity that they can demonstrate a valid public safety purpose in an enumerated Role. Where a Private Entity operates NG9-1-1 services for a Public Safety Entity, the NG9-1-1 Certificate will normally be issued to that Public Safety Entity, even when a Private Organization operates as a Legal Agent of a Public Safety Entity (for example, contractors). An Applicant qualifies as a Private Organization if:

1. The Private Entity serves a public safety purpose in an enumerated Role; and
2. The Private Entity can prove Sponsorship; and
3. The entity's Jurisdiction of Incorporation, Registration, Charter, License, and/or its Place of Business is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
4. The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

Items 1-4 above MAY be waived if the issuance of such certificates is expressly approved by the applicable MA or its Legal Agent.

5.5.3 Public Safety Entity Subjects

Most NG9-1-1 Certificates will be issued to Public Safety Entities, unless special circumstances are approved by NIOC or the appropriate MA. An Applicant qualifies as a Public Safety Entity if:



1. The entity's legal existence was established by the political subdivision in which the entity operates;
2. The entity is directly involved in public safety operations, such as operating an NG9-1-1 PSAP or NG9-1-1 Core Services network, directly responding to incidents and/or providing material support for such activities;
3. The entity can demonstrate that it serves in a Role enumerated in i3 or the applicable registry(ies);
4. The entity is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
5. The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

5.5.4 Business Entity Subjects

Business Entities are subject to the same requirements as Private Organizations.

5.5.5 Non-Commercial Entity Subjects

Non-Commercial Entities are subject to the same requirements as Private Organizations.

632 6 NG9-1-1 Certificate Content and Profile
633 Per the CP, except as elaborated below.

634 **6.1** Issuer Information
635 Per the CP; otherwise, no stipulation.

636 **6.2** Subject Distinguished Name Fields
637 Per the CP; otherwise, no stipulation.

638 **6.3** Subject Common Name Field
639 Per the CP; otherwise, no stipulation.

640 **6.4** Subject Jurisdiction of Incorporation or Registration Field
641 Per the CP; otherwise, no stipulation.

642 6.4.1 Subject Registration Number Field
643 Per the CP; otherwise, no stipulation.

644 6.4.2 Subject Organizational Unit Name Field
645 Per the CP; otherwise, no stipulation.

646 **6.5** Subject Organization Identifier Field
647 Per the CP; otherwise, no stipulation.

648 **6.6** Other Subject Attributes
649 Per the CP; otherwise, no stipulation.

650 **6.7** Certificate Policy Identification
651 Per the CP.

652 **6.8** Certificate Policy Identification Requirements
653 Per the CP; otherwise, no stipulation.

654 **6.9** Subscriber Certificates
655 Per the CP; otherwise, no stipulation.

656 **6.10** Root CA Certificates
657 Per the CP.¹²

¹² The Root CA is the PCA.

658 **6.11** Subordinate ICA Certificates
659 Per the CP; otherwise, no stipulation.

660 **6.12** Subscriber Certificates
661 Per the CP; otherwise, no stipulation.

662 **6.13** Maximum Validity Period For Certificates
663 Per the CP; otherwise, no stipulation.

664 **6.14** Subscriber Public Key
665 Per the CP; otherwise, no stipulation.

666 **6.15** Certificate Serial Number
667 Per the CP; otherwise, no stipulation.

668 **6.16** Additional Technical Requirements for Validating Certificates
669 Per the CP; otherwise, no stipulation.

670 **6.17** Certificate Extensions

671 6.17.1 Subject Alternative Name Extension
672 Certificate field: subjectAltName:OtherName
673 Required/Optional: Required
674 Contents: This extension MUST conform to the requirements of the NIOC CP.
675 The CA SHALL validate that the information in the Subject Alternative Name Extension is correct
676 according to procedures allowed under this Validation Policy.

677 6.17.2 Organization Identifier Field
678 The NENA Registry System maintains sub-OIDs for the CP (as requested in the CP)¹³ under an
679 Internet Assigned Numbers Authority (IANA)-registered Private Enterprise Number for NIOC.¹⁴

680 **7 NG9-1-1 Certificate Request Requirements**

681 **7.1** General Requirements

682 **7.2** Documentation Requirements
683 No stipulation.

¹³ See the CP.

¹⁴ 55670, see <https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>.



684 **7.3** Role Requirements

685 The following Applicant roles, as assigned by the Principal Individual, are required for the
686 issuance of an NG9-1-1 Certificate.

- 687 1. Certificate Requester: The NG9-1-1 Certificate Request MUST be submitted by an
688 authorized Certificate Requester. A Certificate Requester is a natural person who is
689 either the Applicant, employed by the Applicant, an authorized Legal Agent who has
690 express authority to represent the Applicant, or a third party that completes and submits
691 an NG9-1-1 Certificate Request on behalf of the Applicant. If the Subscriber and the CA
692 are affiliated, then the Certificate Requester Terms of Use applicable to the requested
693 NG9-1-1 Certificate MUST be acknowledged and agreed to by the Applicant or their
694 authorized representative.
- 695 2. Certificate Approver: The NG9-1-1 Certificate Request MUST be approved by an
696 authorized Certificate Approver. A Certificate Approver is a natural person who is either
697 the Applicant, employed by the Applicant, or an authorized Legal Agent who has express
698 authority to represent the Applicant to (i) act as a Certificate Requester and to authorize
699 other employees or third parties to act as a Certificate Requester, and (ii) to approve
700 NG9-1-1 Certificate Requests submitted by other Certificate Requesters.
- 701 3. Contract Signer: A Subscriber Agreement applicable to the requested NG9-1-1
702 Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a
703 natural person who is either the Applicant, employed by the Applicant, or an authorized
704 Legal Agent who has express authority to represent the Applicant, and who has
705 authority on behalf of the Applicant to sign Subscriber Agreements.

706 The Applicant MAY authorize one individual to occupy two or more of these roles. The
707 Applicant MAY authorize more than one individual to occupy any one of these roles.

708 **7.4** Requirements for Subscriber Agreement and Terms of Use

709 Section 9.6.3 of the NG9-1-1 CP applies equally to NG9-1-1 Certificates. In cases where the
710 Certificate Request does not contain all necessary information about the Applicant, the CA
711 MUST additionally confirm the data with the Certificate Approver or Contract Signer rather than
712 the Certificate Requester.

713 **7.5** NG9-1-1 Certificate Request Requirements

714 The Certificate Request requirements in Sections 3 and Section 4 of the NG9-1-1 CP¹⁵ apply
715 equally to NG9-1-1 Certificates subject to the requirements of these Guidelines.

¹⁵ See the CP as of 12 May 2021.

716 8 Verification Requirements

717 **8.1** General Overview

718 This part of the Guidelines sets forth Verification Requirements and Acceptable Methods of
719 Verification for each such Requirement.

720 **8.2** Verification Requirements for NG9-1-1 Certificate Types

721 Before issuing an NG9-1-1 Certificate, the CA, RA or LRA MUST ensure that all Subject
722 organization information to be included in the NG9-1-1 Certificate Subject Alternative Name
723 extension conforms to the requirements of, and is verified in accordance with, these Guidelines
724 and matches the information confirmed and documented by the CA.

725 8.2.1 Verification of the Root Certificate

726 Per the CP.

727 8.2.2 Verification of ICA Certificates

728 Per the CP.

729 8.2.3 Verification of Agency Certificates

730 All Verification Requirements in 8, except for 8.6 when it does not apply in accordance with the
731 CP.

732 8.2.4 Verification of all Other Certificates

733 Verification requirements under 8.4, 8.6, 8.12 and 8.15.

734 **8.3** Verification Methods

735 8.3.1 Acceptable Methods of Verification – Overview

736 The CA is responsible for ensuring the completion of all verification steps reasonably necessary
737 to satisfy each of the requirements set forth in the subsections below. In most cases, the RA or
738 LRA will perform the actual Validation. The CA is ultimately responsible for taking any additional
739 verification steps that may be reasonably necessary under the circumstances to satisfy the
740 applicable Verification Requirement.

741 **8.4** Verification of Role

742 To verify a Subject's Role, the RA or LRA MUST do the following:

1. Validate that the requested Roles attested for the Subject conforms to Roles enumerated in the appropriate registry(ies).^{16 17}

8.5 Verification of Agency Identity

For Agency Certificates, a Subject's Agency will be in the format of a Fully-Qualified Domain Name (FQDN). To verify a Subject's Agency for an Agency Certificate, the RA or LRA MUST confirm control of the FQDN using one of the following methods:

8.5.1 DNS Change

The RA or LRA may confirm the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either:

1. An Authorization Domain Name; or
2. an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after

1. 30 days of the Applicant's Attestation; or
2. if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate as specified in the applicable CPS.

Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

8.5.2 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN. This may confirm the Applicant's control of the IP Address by:

1. Observing an agreed-upon change in the IP address associated with an A or AAAA record attested by the Applicant within:
 - a. 30 days of the Applicant's attestation; or
 - b. if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate.

¹⁶ For Agency Certificates, the Agency must have one more or Roles from the Agency Roles registry; and must also have one or more Roles from the urn:emergency:service:responder registry or the appropriate subregistry(ies). See i3 at Section 10.

¹⁷ For Agent Certificates, the Agent must have one or more Roles from the Agent Roles registry or the appropriate subregistry(ies). See *Id.*



772 Once the FQDN has been validated using this method, the CA MAY NOT also issue Certificates
773 for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a
774 separate validation for that FQDN using an authorized method.

775 8.5.3 Agreed-**Upon Change to Website v2**

776 Confirming the Applicant's control over the FQDN by verifying that the Request Token or
777 Random Value is contained in the contents of a file or website at the FQDN in a manner
778 specified by the RA or LRA.

- 779 1. The entire Request Token or Random Value MUST NOT appear in the request used
780 to retrieve the file or access the website, and
- 781 2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx
782 HTTP status code must be received).

783 The file or website containing the Request Token or Random Number:

- 784 1. MUST be located on the Authorization Domain Name, and
- 785 2. SHOULD be located under the "/.well-known/pki-validation" directory, and
- 786 3. MUST be retrieved via either the "http" or "https" scheme, and
- 787 4. MUST be accessed over an Authorized Port.

788 If the CA follows redirects, the following apply:

- 789 1. Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as
790 defined in RFC 7231,¹⁸ Section 6.4, or a 308 HTTP status code response, as defined in
791 RFC 7538,¹⁹ Section 3. Redirects MUST be to the final value of the Location HTTP
792 response header, as defined in RFC 7231, Section 7.1.2.
- 793 2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
- 794 3. Redirects MUST be to resource URLs accessed via Authorized Ports.

795 If a Random Value is used, then:

- 796 1. The CA MUST provide a Random Value unique to the certificate request.
- 797 2. The Random Value MUST remain valid for use in a confirming response for no more than
798 30 days from its creation. The CPS MAY specify a shorter validity period for Random
799 Values, in which case the CA MUST follow its CPS.

800 Note: CAs MUST NOT issue Certificates for other FQDNs that end with all the labels of the
801 validated FQDN unless the CA performs a separate validation for that FQDN using an authorized
802 method. This method is NOT suitable for validating Wildcard Domain Names.

¹⁸ <https://datatracker.ietf.org/doc/html/rfc7231>

¹⁹ <https://datatracker.ietf.org/doc/html/rfc7538>



803 8.5.4 Agreed-**Upon Change to Website - ACME**

804 Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using
805 the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555.²⁰ The following are
806 additive requirements to RFC 8555.

807 The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP
808 status code must be received). The token (as defined in RFC 8555, Section 8.3) MUST NOT be
809 used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for
810 Random Values, in which case the CA MUST follow its CPS.

811 If the CA follows redirects, the following apply:

- 812 1. Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as
813 defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC
814 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response
815 header, as defined in RFC 7231, Section 7.1.2.
- 816 2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
- 817 3. Redirects MUST be to resource URLs accessed via Authorized Ports.

818 Note: CAs MUST NOT issue Certificates for other FQDNs that end with all the labels of the
819 validated FQDN unless the CA performs a separate validation for that FQDN using an authorized
820 method. This method is NOT suitable for validating Wildcard Domain Names.

821 8.5.5 Any Other Method

822 Any other method not included in this section SHALL NOT be used.

²⁰ <https://datatracker.ietf.org/doc/html/rfc8555>



823 **8.6 Verification of Owner**

824 The RA or LRA MUST confirm the identity of the Owner²¹ by an electronic signature provided by
825 an Agency Certificate whose FQDN matches the "Owner" field. The signing of the Certificate
826 Signing Request by the Owner is sufficient to validate the Agent.

827 When the Owner is a CA, the fact that the Certificate is issued by the CA is sufficient to validate
828 the Owner as being the CA.

829 Private Entities SHOULD have a sponsor that is a Public Safety Entity that is the Owner for its
830 Agency, Agent, Element and Service Certificates. If a Private Entity does not have a sponsor, it
831 MUST have an Agency Certificate approved by the appropriate MA for that CPS.

832 **8.6.1 Verification of Owner for Agency Certificates**

833 Per the CP.

834 **8.7 Verification of Applicant's Legal Existence and Identity**

835 **8.7.1 Verification Requirements**

836 To verify the Applicant's legal existence and identity, the RA or LRA MUST do the following:

- 837 1. Legal Existence: Verify that the Applicant is a legally recognized Public Safety Entity or
838 a Private Entity with a valid public safety purpose, in existence and validly formed (e.g.,
839 enabling statute, ordinance, municipal incorporation, joint powers agreement or similar;
840 or articles of incorporation, business registration or similar) in the Applicant's Jurisdiction
841 of Incorporation.
- 842 2. Organization Name: Verify that the Applicant's formal legal name in the Applicant's
843 jurisdiction matches the Applicant's name in the NG9-1-1 Certificate Request.
- 844 3. Registration Number: For Private Entities, obtain the specific Registration Number
845 assigned to the Applicant in the Applicant's Jurisdiction of Incorporation or Registration.
846 Where the Applicant does not have a Registration Number, the CA SHALL obtain the
847 Applicant's date of Incorporation or Registration.
- 848 4. Registered Agent: Private Entities that obtain a Certificate SHALL NOT do so through a
849 legal Registered Agent.
- 850 5. Public Safety Function: Verify that the Applicant or the element which they control is
851 performs a legitimate public safety function required for NG9-1-1, such as by validating an
852 enumerated Role, or for Private Entities, reviewing available information about the
853 company's mission statement and business purposes.
- 854 6. Principal Individual: Verify the identity of the identified Principal Individual per section
855 8.7.2.
- 856 7. Agency Identity: Verify the agency identity per section 8.5.

²¹ Per the CP at 7.1.2.11; an Agency Certificate may not have an Owner.

857 8.7.2 Acceptable Method of Verification

- 858 1. Private Entity Subjects: Unless verified under subsection (4), all items listed in
859 Section 8.2 MUST be verified directly with the Appropriate Authority. Such verification MAY
860 be through direct contact with the Appropriate Authority in person or via mail, e-mail,
861 Web address, or telephone, using an address or phone number obtained directly from a
862 QGIS, Incorporating or Registration Agency, or from a QIIS.
- 863 2. Public Safety Entity Subjects: Unless verified under subsection (4), all items listed in
864 Section 8.7.1 MUST either be verified directly with, or obtained directly from, one of the
865 following:
- 866 a. a QGIS in the political subdivision in which such Public Safety Entity operates;
 - 867 b. a superior governing Public Safety Entity in the same political subdivision as the
868 Applicant (e.g., an elected sheriff may verify the legal existence of functions within
869 their own sheriff's office), or
 - 870 c. from a judge that is an active member of the federal, state, or local judiciary
871 within that political subdivision.

872 Any communication from a judge SHALL be verified in the same manner as is used for verifying
873 factual assertions that are asserted by an attorney.

874 Such verification MAY be by direct contact with the appropriate Public Safety Entity in person or
875 via mail, e-mail, Web address, or telephone, using an address or phone number obtained from
876 a QIIS.

- 877 1. Principal Individual: A Principal Individual MUST be validated in a face-to-face setting.
878 The CA MAY rely upon a face-to-face validation of the Principal Individual performed by
879 the RA or LRA, provided that the CA has evaluated the validation procedure and
880 concluded that it satisfies the requirements of the Guidelines for face-to-face validation
881 procedures. Where no face-to-face validation was conducted by the RA, or the RA's face-
882 to-face validation procedure does not satisfy the requirements of the Guidelines, the CA
883 SHALL perform face-to-face validation.

- 884 a. Face-To-Face Validation: The face-to-face validation MUST be conducted
885 before either an employee or Legal Agent of the CA, an RA or an LRA. The face-
886 to-face validation MAY be performed virtually (e.g., via video conference). The
887 Principal Individual(s) MUST present the following documentation directly to the
888 RA or LRA:

- 889 i. A Personal Statement that includes the following information:

- 890 1. Full name or names by which the person is, or has been, known
891 (including all other names used)
- 892 2. Official Title, including Agency affiliation;
- 893 3. Address at which the person can be located, and



- 894 4. An affirmation that all of the information contained in the Certificate
895 Request is true and correct.
- 896 ii. The RA or LRA MUST:
- 897 1. Verify the Principal Individual's full name, official title and Agency
898 affiliation through a QGIS, QIIS, government-issued identification or
899 equivalent.
- 900 2. Attest to the signing of the Personal Statement and the identity of
901 the signer; and
- 902 b. Verification of Validator: The CA MUST verify that the RA or LRA actually did
903 perform the services and did attest to the identity of the Individual.

904 **8.8 Verification of Applicant's Physical Existence – Place of Operations**

905 **8.8.1 Verification Requirements**

906 To verify the Applicant's physical existence and business presence, the CA, the RA or LRA MUST
907 verify that the physical address provided by the Applicant is an address where the Applicant
908 conducts operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such
909 as an address for a Legal Agent of the organization) and is the address of the Applicant's Place
910 of Operations.

911 **8.8.2 Acceptable Methods of Verification**

912 Applicants SHALL provide a Place of Operations and this SHALL be validated by one of the
913 following:

- 914 a. For Applicants listed at the same Place of Operations address in the current
915 version of either at least one QGIS (other than that used to verify legal existence),
916 QIIS or QTIS, the CA, RA or LRA MUST confirm that the Applicant's address, as
917 listed in the NG9-1-1 Certificate Request, is a valid address for the Applicant by
918 reference to such QGIS, QIIS, or QTIS, and MAY rely on the Applicant's
919 representation that such address is its Place of Operations;
- 920 b. For Applicants who are not listed at the same Place of Operations address in the
921 current version of either at least one QIIS or QTIS, the CA, the RA or LRA MUST
922 confirm that the address provided by the Applicant in the NG9-1-1 Certificate
923 Request is the Applicant's address, by obtaining documentation of a site visit to the
924 address, which MUST be performed by a reliable individual or firm. The
925 documentation of the site visit MUST:
- 926 i. Verify that the Applicant's Place of Operations is located at the exact
927 address stated in the NG9-1-1 Certificate Request (e.g., via permanent
928 signage, employee confirmation, etc.),



- 929 ii. Identify the type of facility (e.g., official government building, office in a
930 commercial building, etc.) and whether it appears to be a permanent
931 operations location,
- 932 iii. Indicate whether there is a permanent sign (that cannot be moved) that
933 identifies the Applicant, and
- 934 iv. Indicate whether there is evidence that the Applicant is conducting ongoing
935 activities at the site (not that it is just, for example, a mail drop, P.O. box,
936 etc.).

937 **8.9 Verified Method of Communication**

938 8.9.1 Verification Requirements

939 To assist in communicating with the Applicant and confirming that the Applicant is aware of and
940 approves issuance, the RA or LRA MUST verify a telephone number, fax number, email address,
941 or postal delivery address as a Verified Method of Communication with the Applicant.

942 8.9.2 Acceptable Methods of Verification

943 To verify a Verified Method of Communication with the Applicant, the RA or LRA MUST:

- 944 1. Verify that the Verified Method of Communication belongs to the Applicant, or a
945 Parent/Subsidiary or Affiliate of the Applicant, by matching it with: a QGIS, QTIS, or
946 QIIS; and
- 947 2. Confirm the Verified Method of Communication by using it to obtain an affirmative
948 response sufficient to enable a reasonable person to conclude that the Applicant, or a
949 Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified
950 Method of Communication.

951 8.9.3 **Verification of Applicant's Operational Existence**

952 8.9.4 Verification Requirements

953 The CA, RA or LRA MUST verify that the Applicant does engage in its stated Role by verifying
954 the Applicant's, or Affiliate/Parent/Subsidiary's, operational existence. The CA, RA or LRA MAY
955 rely on its verification of a Public Safety Entity's legal existence under Section 8.2 as verification
956 of its operational existence.

957 1. Acceptable Methods of Verification

- 958 a. Private Entity Subjects: Verification MUST be through a QGIS or QIIS.
- 959 b. Public Safety Entity Subjects: The Applicant's legal existence MUST either be
960 verified directly with, or obtained directly from, one of the following:
- 961 i. a QGIS in the political subdivision in which such Public Safety Entity
962 operates;



- ii. a superior governing Public Safety Entity in the same political subdivision as the Applicant (e.g., an elected sheriff may verify the legal existence of functions within their own sheriff's office), or
- iii. from a judge that is an active member of the federal, state, or local judiciary within that political subdivision.

Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an attorney.

Such verification MAY be by direct contact with the appropriate Public Safety Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a QIIS or QGIS.

8.10 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

8.10.1 Verification Requirements

For both the Contract Signer and the Certificate Approver, the RA or LRA MUST verify the following.

1. Name, Title and Agency: The name and title of the Contract Signer and the Certificate Approver, as applicable. The RA MUST also verify that the Contract Signer and the Certificate Approver are Legal Agents representing the Applicant.
2. Signing Authority of Contract Signer: That the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.
3. Authority of Certificate Approver: Through a source other than the Certificate Approver their self, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the NG9-1-1 Certificate Request, to:
 - a. Submit, and, if applicable, authorize a Certificate Requester to submit, the NG9-1-1 Certificate Request on behalf of the Applicant; and
 - b. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the NG9-1-1 Certificate; and
 - c. Approve NG9-1-1 Certificate Requests submitted by a Certificate Requester.

8.10.2 Acceptable Methods of Verification – Name, Title and Legal Agency

Acceptable methods of verification of the name, title, and Legal Agency status of the Contract Signer and the Certificate Approver include the following:

1. Name and Title: The RA or LRA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable



assurance that a person claiming to act in such a role is in fact the named person designated to act in such role.

2. Legal Agency: The RA or LRA MAY verify the Legal Agency of the Contract Signer and the Certificate Approver using one of the following methods:

a. Contacting the Applicant using a Verified Method of Communication for the Applicant, and obtaining confirmation, either by:

i. Obtaining an Independent Confirmation from the Applicant (as described in Section 8.12.3), or a verified professional letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, has been authorized to act on behalf of the Applicant as its Legal Agent; or

ii. By obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.

b. Via a certification from the Contract Signer (including in a contract between the CA or RA and the Applicant signed by the Contract Signer), provided that the employment or Legal Agent status and Signing Authority of the Contract Signer has been verified.

8.10.3 Acceptable Methods of Verification – Signing Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the Authority of the Certificate Approver, as applicable, include:

1. Resolution: The Signing Authority of the Contract Signer, and/or the Authority of the Certificate Approver, MAY be verified by reliance on a properly authenticated resolution that confirms that the person has been granted such Signing Authority, provided that such resolution (i) is certified by an appropriate officer of the organization (e.g., secretary), and (ii) the can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification;
2. Independent Confirmation from Applicant: The Signing Authority of the Contract Signer, and/or the Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from the Applicant (as described in Section 8.12.3);
3. Contract between CA and Applicant: The Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA, RA or LRA and the Applicant that designates the Certificate Approver with such Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;
4. Prior Equivalent Authority: The Signing authority of the Contract Signer, and/or the Authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.

- 1036 a. Prior Equivalent Authority of a Contract Signer MAY be relied upon for
1037 confirmation or verification of the signing authority of the Contract Signer when
1038 the Contract Signer has executed a binding contract between the CA, RA or LRA
1039 and the Applicant with a legally valid and enforceable seal or handwritten
1040 signature. The CA MUST record sufficient details of the previous agreement to
1041 correctly identify it and associate it with the NG9-1-1 application. Such details
1042 MAY include any of the following:
- 1043 i. Agreement title,
1044 ii. Date of Contract Signer's signature,
1045 iii. Contract reference number, and
1046 iv. Filing location.
- 1047 b. Prior Equivalent Authority of a Certificate Approver MAY be relied upon for
1048 confirmation or verification of the Authority of the Certificate Approver when the
1049 Certificate Approver has performed one or more of the following:
- 1050 i. Under contract to the CA, has served (or is serving) as an LRA for the
1051 Applicant, or
1052 ii. Has participated in the approval of one or more certificate requests, for
1053 certificates issued by the CA and which are currently and verifiably in use
1054 by the Applicant. In this case the CA MUST have contacted the Certificate
1055 Approver by Verified Method of Communication or have accepted a signed
1056 and notarized letter approving the certificate request.
- 1057 5. QIIS or QGIS: The Signing Authority of the Contract Signer, and/or the Authority of the
1058 Certificate Approver, MAY be verified by a QIIS or QGIS that identifies the Contract
1059 Signer and/or the Certificate Approver as an officer, director or other senior official of the
1060 Applicant.
- 1061 6. **Contract Signer's Representation/Warranty:** Provided that the RA or LRA verifies
1062 that the Contract Signer is an employee or Legal Agent of the Applicant, the CA MAY rely
1063 on the signing authority of the Contract Signer by obtaining a duly executed
1064 representation or warranty from the Contract Signer that includes the following
1065 acknowledgments:
- 1066 a. That the Applicant authorizes the Contract Signer to sign the Subscriber
1067 Agreement on the Applicant's behalf,
1068 b. That the Subscriber Agreement is a legally valid and enforceable agreement,
1069 c. That, upon execution of the Subscriber Agreement, the Applicant will be bound by
1070 all of its terms and conditions, and
1071 d. That serious consequences attach to the misuse of an NG9-1-1 certificate.

8.10.4 Pre-Authorized Certificate Approver

Where the CA and Applicant contemplate the submission of multiple future NG9-1-1 Certificate Requests, then, after the RA or LRA:

1. Has verified the name and title of the Contract Signer and that he/she is an employee or Legal Agent of the Applicant; and
2. Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Section 8.10; then

The CA, RA or LRA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise Authority with respect to each future NG9-1-1 Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

Such an agreement MUST provide that the Applicant shall be obligated under the Subscriber Agreement for all NG9-1-1 Certificates issued at the request of, or approved by, such Certificate Approver(s) until NG9-1-1 Certificate Request Authority is Revoked, and MUST include mutually agreed-upon provisions for:

- a. authenticating the Certificate Approver when NG9-1-1 Certificate Requests are approved,
- b. periodic re-confirmation of the NG9-1-1 Authority of the Certificate Approver,
- c. secure procedures by which the Applicant can notify the CA that the NG9-1-1 Certificate Request Authority of any such Certificate Approver is Revoked, and
- d. such other appropriate precautions as are reasonably necessary.

8.11 Verification of Signature on Subscriber Agreement and NG9-1-1 Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized NG9-1-1 Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The NG9-1-1 Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Section 8.10.4 of these Guidelines. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the NG9-1-1 Certificate Request. In all cases, applicable signatures MUST be legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or NG9-1-1 Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or NG9-1-1 Certificate Request), that binds the Applicant to the terms of each respective document.

8.11.1 Verification Requirements

1. Signature: The CA, RA or LRA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each NG9-1-1 Certificate Request in a manner that makes it reasonably certain that the person named as the Contract Signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.
2. Approval Alternative: In cases where an NG9-1-1 Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the NG9-1-1 Certificate Request by a Certificate Approver in accordance with the requirements of Section 8.12 can substitute for authentication of the signature of the Certificate Requester on such NG9-1-1 Certificate Request.

8.11.2 Acceptable Methods of Signature Verification

Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include the following:

1. Contacting the Applicant using a Verified Method of Communication for the Applicant, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that they did sign the applicable document on behalf of the Applicant;
2. A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with these Guidelines, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response through a Verified Method of Communication from someone who identifies themselves as such person confirming that they did sign the applicable document on behalf of the Applicant; or
3. Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate.

8.12 Verification of Approval of NG9-1-1 Certificate Request

8.12.1 Verification Requirements

In cases where an NG9-1-1 Certificate Request is submitted by a Certificate Requester, before the CA issues the requested NG9-1-1 Certificate, the CA, RA or LRA MUST verify that an authorized Certificate Approver reviewed and approved the NG9-1-1 Certificate Request.

8.12.2 Acceptable Methods of Verification

Acceptable methods of verifying the Certificate Approver's approval of an NG9-1-1 Certificate Request include:



1. Contacting the Certificate Approver using a Verified Method of Communication for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the NG9-1-1 Certificate Request;
2. Notifying the Certificate Approver that one or more new NG9-1-1 Certificate Requests are available for review and approval at a designated access-controlled and secure website, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site which shall be at least two-factor authentication; or
3. Verifying the signature of the Certificate Approver on the NG9-1-1 Certificate Request in accordance with Section 8.11.2 of these Guidelines.

8.12.3 Independent Confirmation from Applicant

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the NG9-1-1 Authority of a Certificate Approver, etc.) that is:

1. Received by the RA or LRA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the Appropriate Authority to confirm such a fact, and who represents that he/she has confirmed such fact;
2. Received by the RA or LRA in a manner that authenticates and verifies the source of the confirmation; and
3. Binding on the Applicant.

An Independent Confirmation from the Applicant MAY be obtained via the following procedure:

1. Confirmation Request: The RA or LRA MUST initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:
 - a. Addressee: The Confirmation Request MUST be directed to:
 - i. A position within the Applicant's organization that qualifies as a Confirming Person (e.g., an elected official, an individual serving in an official role in a Public Safety Entity, an Individual appointed by an elected official, CSO, Director, etc.) and is identified by name and title in a current QGIS, QIIS, QTIS, or by contacting the Applicant using a Verified Method of Communication; or
 - ii. A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's human resources department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Guidelines, or through publicly-available records).

b. Means of Communication: The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:

i. By paper mail addressed to the Confirming Person at:

1. The address of the Applicant's Place of Operations as verified by the CA in accordance with these Guidelines, or
2. The address for such Confirming Person specified in a current QGIS, QTIS, QIIS, or

ii. Via a method of communication as listed in 8.11 to the Confirming Person for such person listed in a current QGIS, QTIS, QIIS.

2. Confirmation Response: The RA or LRA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the RA or LRA by any method of communication as listed in 8.11 so long as the Confirming Person can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.
3. The RA or LRA MAY rely on a verified Confirming Person to confirm their own contact information. The RA or LRA MAY rely on this verified contact information for future correspondence.

8.12.4 Qualified Independent Information Source (QIIS)

A Qualified Independent Information Source (QIIS) is a regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if it is determined that:

1. Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and
2. The database provider updates its data on at least an annual basis.

The RA or LRA SHALL document which QIIS it uses to verify any fact at issue. The LA or LRA SHALL use a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use.

- 1207 8.12.5 Qualified Government Information Source (QGIS)
- 1208 A Qualified Government Information Source (QGIS) is a regularly-updated and current, publicly
- 1209 available, database designed for the purpose of accurately providing the information for which it
- 1210 is consulted, and which is generally recognized as a dependable source of such information
- 1211 provided that it is maintained by a Public Safety Entity or a unit of government. The RA or LRA
- 1212 SHALL document which QGIS it uses to verify any fact at issue. Nothing in these Guidelines
- 1213 shall prohibit the use of third-party vendors to obtain the information from the Public Safety
- 1214 Entity or a unit of government provided that the third party obtains the information directly
- 1215 from the Public Safety Entity or a unit of government.
- 1216 8.12.6 Qualified Government Tax Information Source (QTIS)
- 1217 A Qualified Government Tax Information Source is a QGIS that specifically contains tax
- 1218 information relating to Private Organizations, Business Entities or Individuals (e.g., the IRS in
- 1219 the United States).
- 1220 **8.13 Other Verification Requirements**
- 1221 8.13.1 High Risk Status
- 1222 No stipulation.
- 1223 8.13.2 Denied Lists and Other Legal Unapproved Lists
- 1224 1. Verification Requirements: The RA or LRA MUST verify whether the Applicant, the
- 1225 Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation,
- 1226 Registration, or Place of Operations:
- 1227 a. Is identified on any government denied list, list of prohibited persons, or other
- 1228 reputable list that prohibits engaging in business or other specified activities with
- 1229 such organization or person under the laws, regulations, technical standard or
- 1230 best practice, of CA's jurisdiction(s) of operation; or
- 1231 b. Has its Jurisdiction of Incorporation, Registration, or Place of Operations in any
- 1232 country with which the laws of the CA's jurisdiction prohibit doing business or
- 1233 other specified activities.
- 1234 The CA MUST NOT issue any NG9-1-1 Certificate to the Applicant if the Applicant, the Contract
- 1235 Signer, or Certificate Approver or if the Applicant's Jurisdiction or Registration or Place of
- 1236 Operations is on any such list.
- 1237 2. Acceptable Methods of Verification: The RA or LRA MUST take reasonable steps to
- 1238 verify with the following lists and regulations:
- 1239 a. If the CA has operations in the U.S., the CA MUST take reasonable steps to verify with
- 1240 the following US Government denied lists and regulations:
- 1241 i. United States Bureau of Industry and Security (BIS) Denied Persons List -
- 1242 <http://www.bis.doc.gov/dpl/thedeniallist.asp>

- 1243 ii. BIS Denied Entities List - [https://www.bis.doc.gov/index.php/policy-](https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list)
1244 [guidance/lists-of-parties-of-concern/entity-list](https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list)
1245 iii. US Treasury Department List of Specially Designated Nationals and Blocked
1246 Persons - <http://www.treas.gov/ofac/t11sdn.pdf>
1247 iv. US Government export regulations
1248 b. If the CA has operations in any other country, the CA MUST take reasonable steps
1249 to verify with all equivalent denied lists and export regulations (if any) in such other
1250 country.

1251 8.13.3 Parent /Subsidiary /Affiliate Relationship

1252 An RA or LRA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or
1253 Affiliate, when allowed under these Guidelines, MUST verify the Applicant's relationship to the
1254 Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to
1255 the Parent, Subsidiary, or Affiliate include the following:

- 1256 1. QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or
1257 Affiliate is identified in a QIIS or QGIS;
- 1258 2. Independent Confirmation from the Parent, Subsidiary, or Affiliate: An RA or LRA MAY
1259 verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by
1260 obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate
1261 (as described in Section 8.12.3);
- 1262 3. Contract between CA or RA and Parent, Subsidiary, or Affiliate: An RA or LRA MAY verify
1263 the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a
1264 contract between the CA, or the RA and the Parent, subsidiary, or Affiliate that designates
1265 the Certificate Approver with such NG9-1-1 Authority, provided that the contract is signed
1266 by the Contract Signer and provided that the Legal Agency and Signing Authority of the
1267 Contract Signer have been verified;
- 1268 4. Verified Professional Letter: An RA or LRA MAY verify the relationship between an Applicant
1269 and a Parent, Subsidiary, or Affiliate by relying on a Verified Professional Letter; or
- 1270 5. Resolution: An RA or LRA MAY verify the relationship between an Applicant and a Subsidiary
1271 by relying on a properly authenticated resolution that approves creation of the Subsidiary
1272 or the Applicant, provided that such resolution is (i) certified by the appropriate officer (e.g.,
1273 secretary), and (ii) the CA can reliably verify that the certification was validly signed by such
1274 person, and that such person does have the requisite authority to provide such certification.

1275 **8.14** Final Cross-Correlation and Due Diligence

1276 For NG9-1-1 Certificates:

- 1277 1. The results of the verification processes and procedures outlined in these Guidelines are
1278 intended to be viewed both individually and as a group. Thus, after all of the verification
1279 processes and procedures are completed, the RA or LRA MUST have a person who is not
1280 responsible for the collection of information review collection of all of the information and



documentation assembled in support of the NG9-1-1 Certificate Application and look for discrepancies or other details requiring further explanation.

2. The RA or LRA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, QIISeS, and/or other sources of information, as necessary, to resolve discrepancies or details that require further explanation.
3. The CA MUST refrain from issuing an NG9-1-1 Certificate until the entire corpus of information and documentation assembled in support of the NG9-1-1 Certificate Request is such that issuance of the NG9-1-1 Certificate will not communicate factual information that the CA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA MUST decline the NG9-1-1 Certificate Request and SHOULD notify the Applicant accordingly.
4. The normal operating language of the CA SHALL be American English. When the Applicant does not possess the language skills necessary to operate in the normal operating language of the CA, a CA MAY:
 - a. Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or
 - b. When the CA has utilized the services of an RA or LRA, the CA MAY rely on the language skills of the RA or LRA to perform the Final Cross-Correlation and Due Diligence. Notwithstanding the foregoing, prior to issuing the NG9-1-1 Certificate, the CA MUST review the work completed by the RA or LRA and determine that all requirements have been met.

8.15 Requirements for Re-use of Existing Documentation

For each NG9-1-1 Certificate Request, including requests to renew existing NG9-1-1 Certificates, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the NG9-1-1 Certificate is still accurate and valid. This section sets forth the age limitations on the use of documentation collected by the CA.

8.15.1 Validation For Existing Subscribers

If an Applicant has a currently valid NG9-1-1 Certificate issued by the CA, a CA MAY rely on its prior authentication and verification of information that has been verified before issuing the NG9-1-1 Certificate in accordance with the stipulations in the CPS for the CA.

8.15.2 Re-issuance Requests

Per the CP.



8.15.3 Age of Validated Data

1. Except when permitted otherwise in Section 8.15.1, the age of all data used to support issuance of an NG9-1-1 Certificate (before revalidation is required) SHALL NOT exceed the following limits:
 - a. Legal existence and identity – three years;
 - b. Assumed name – three years;
 - c. Address of Place of Operations – three years;
 - d. Verified Method of Communication – thirteen months;
 - e. Operational existence – three years;
 - f. Agency Identity – three years;
 - g. Name, Title, Agency, and Authority – three years, unless a contract with the CA specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of roles until Revoked by the Applicant or CA, or until the contract expires or is terminated.
2. The periods set forth above SHALL begin to run on the date the information was collected by the CA.
3. The CA MAY reuse a previously submitted NG9-1-1 Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single NG9-1-1 Certificate Request in support of multiple NG9-1-1 Certificates containing the same Subject to the extent permitted under Sections 8.9 and 8.10.
4. The CA MUST repeat the verification process required in these Guidelines for any information obtained outside the time limits specified above except when permitted otherwise under section 8.15.1.

9 Certificate Issuance by a Root CA

Per the CP.

9.1.1 Identity and Background Verification

Prior to the commencement of employment of any person by the CA, RA or LRA for engagement in the processes under these Guidelines, whether as an employee, Legal Agent, or an independent contractor of the CA, RA or LRA, the CA, RA or LRA MUST:

1. Verify the Identity of such Person: Verification of identity MUST be performed through:
 - a. The personal (physical or virtual) presence of such person before trusted persons who perform human resource or security functions, and
 - b. The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licenses); and
2. Verify the Trustworthiness of such person: Verification of trustworthiness SHALL include background checks, which address at least the following, or their equivalent:
 - a. Confirmation of previous employment,
 - b. Check of professional references;



- c. Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed; and
- d. For Public Safety Entities, that existing background check procedures for identifying the trustworthiness of employees is sufficient to meet the requirements of these Guidelines.
3. In the case of employees already in the employ of the CA, RA or LRA at the time of adoption of these Guidelines whose identity and background has not previously been verified as set forth above, the CA, RA or LRA SHALL conduct such verification within three months of the date of adoption of these Guidelines under the applicable CPS.

10 Certificate Revocation and Status Checking

Per the requirements in the PCA CP, the Certificate Revocation and Status Checking Requirements apply equally to all NG9-1-1 Certificates.

11 Employee and third party issues

11.1 Trustworthiness and Competence

11.1.1 Training and Skills Level

No Stipulation.

11.1.2 Separation of Duties

Per the CP.

11.2 Delegation of Functions to Registration Authorities and Subcontractors

11.2.1 General

The CA MAY delegate the performance of all or any part of a requirement of these Guidelines to an Affiliate, RA or LRA, or subcontractor, provided that the process employed by the CA fulfills all of the requirements of these Guidelines.

The party that so delegates any such performance remains wholly responsible for ensuring that all requirements of this document and the CP are met.

11.2.2 Local Registration Authority (LRA)

The RA for a CA MAY authorize the Subject of a valid NG9-1-1 Certificate to perform the RA function and authorize the CA to issue NG9-1-1 Certificates at the Tier controlled by the Subject's issuing CA. In such case, the Subject SHALL be considered an LRA, and the following Requirements SHALL apply:

1. The LRA SHALL NOT authorize the CA to issue Certificates at a Tier other than for the Tier that the CA directly issues Certificates.
2. In all cases, the LRA MUST be an organization verified by the RA in accordance with these Guidelines.



- 1389 3. The RA MUST monitor compliance with these Guidelines by the LRA.
1390 4. The Final Cross-Correlation and Due Diligence requirements of these Guidelines equally
1391 apply to the LRA; and
1392 5. The audit requirements of these Guidelines SHALL apply to the LRA, except in the case
1393 where the CA maintains control over the Private Key used to issue the Certificates
1394 authorized by the LRA, in which case, the LRA MAY be exempted from the audit
1395 requirements.

1396 11.2.3 Guidelines Compliance Obligation

1397 In all cases, any delegate having delegated Authority must be contractually obligated to the
1398 delegator to comply with all applicable requirements in these Guidelines and to perform them
1399 as required of the delegator itself. The delegator SHALL enforce these obligations and internally
1400 audit each of their delegate’s compliance with these Requirements on an annual basis.

1401 11.2.4 Allocation of Liability

1402 Per the CP.

1403 12 Data Records

1404 Per the CP.

1405 13 Data Security

1406 Per the CP.

1407 14 Audit

1408 Per the CP.

1409 **14.1** Eligible Audit Schemes

1410 Per the CP.

1411 **14.2** Per the CP Audit Period

1412 Per the CP.



14.3 Audit Record

Per the CP.

14.4 Pre-Issuance Readiness Audit

No stipulation.

14.5 Per the CP Regular Self Audits

Per the CP.

14.6 Per the CP Auditor Qualification

Per the CP.

14.7 Per the CP Root CA Key Pair Generation

Per the CP.

15 Liability and Indemnification

Per the CP.

16 Acknowledgements

The National Emergency Number Association (NENA) 9-1-1 Core Services Committee, PCA Certificate Policy Working Group developed this document at the request of the Next Generation 9-1-1 Interoperability Oversight Commission.

Members	Employer
Steve O'Connor, ENP, 9-1-1 Core Services Committee Co-Chair, WG Co-Chair	NG9-1-1 Consulting Services, LLC
Theresa Reese, 9-1-1 Core Services Committee Co-Chair, WG Co-Chair	Ericsson Inc.
Brandon Abley, ENP	NENA
Tom Breen, ENP	SecuLore Solutions, LLC
Guy Caron, ENP	Bell Canada
Mark Fletcher, ENP	911inform, LLC
Suresh Gursahaney	MicroAutomation Inc
Diane Harris, ENP	Zetron Inc
Rob Howard	NYC3 Cyber Command
Chris Kellett	CRTC Emergency Services (9-1-1)
Erik Loberg	GeoComm Inc.
Oscar Marcia	Eonti
Roger Marshall	Comtech Telecommunications Corp.
Steve McMurrer, ENP	Fairfax County VA
William Mertka	Synergem Technologies Inc.
Roman Mezhericher	City of New York
Jackie Mines	Mission Critical Partners, LLC

Members	Employer
Dan Mongrain	Motorola Solutions, Inc.
Michael Newburn	AT&T
Brian Rosen	Consultant
Matthew Schreiner	Mission Critical Partners, LLC
Michael Smith	Equature/DSS Corp.
Tom Soulos	MicroAutomation Inc.
Jamie Taylor	City of Lee's, Summit MO
Fabricio Velez	Nokia
C. A. Patrick Voigt-ENP	Synergem Technologies Inc.
Curtis Wolfenberger Sr	INdigital

Exhibit 8 NIOC PSAP Credentialing Agency PCA Certificate Policy

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

V1.2

06/26/2024

NG9-1-1 Interoperability Oversight Commission (NIOC)



Document Revision History

This document was approved for publication on February 22, 2023 by the NG9-1-1 Interoperability Oversight Commission (NIOC). The following revisions have been made to the original document:

Revision	Date	Remarks
V0.1	2019-11-02	Initial Draft to propose structure and outline Certificate profiles
V0.2	2019-12-07	Draft to review initial Section 1
V0.3	2019-12-08	First pass completed, all Sections 1 - 9
V0.4	2019-12-08	Second pass completed, Section 1
V0.5	2019-12-08	Second pass completed, Section 2
V0.6	2019-12-08	Second pass completed, Section 3
V0.7	2019-12-08	Third pass completed for Sections 1 - 3 – Draft for NENA review
V0.8	2019-12-30	Third pass completed for Sections 4 - 6 – Draft for NENA review
V0.9	2020-01-12	Third pass completed for Sections 7 - 9 – Draft for NENA review
V0.9.1	2020-02-24	Incorporated NENA comments in Sections 1 – 9 and DigiCert comments in Sections 1 – 3. Cleaned Sections 1 – 3.
V0.9.2	2020-03-03	Incorporated NENA comments in Sections 1 – 9 and DigiCert comments in Sections 1 – 6.
V0.9.3	2020-03-16	Incorporated Clean Sections 1 – 6 and NENA and DigiCert comments in Sections 1 – 9.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

V0.9.4	2020-03-16	Clean sections 1 – 6, incorporating comments Sections 6 – 9.
V0.9.5	2020-04-15	Fourth pass, Sections 1- 7
V0.9.6	2020-04-27	Fifth pass, cleanup and scrubbing of CP
V0.9.7	2020-04-29	Cleaned up and scrubbed. Completion of CP.
V0.9.8	2020-08-25	Preliminary Candidate CP Submitted to NIOC for Review.
V0.9.8.1	2020-09-03	Public Review Candidate Submitted to NENA membership for comment.
V0.9.8.1	2020-10-20	Combine edits from Eonti, NIOC and DigiCert.
V0.9.8.2	2020-11-09	Clarifications to responsibilities for NIOC PA and ICA PAs.
V1.0	2020-11-18	Approval by NIOC.
V1.0.1	2021-03-10	Clarifies requirements for <i>otherName</i> field in SAN extension
V1.1	2023-02-22	Changed “Root CA” to “PCA” in the entire document except in a few limited circumstances. Clarified text that describes the role and relationship of the PCA, RA, and PA to Tier 2 ICAs and the ICAs’ PAs and RAs. Clarified text to more explicitly state the role and responsibility of the PCA, PA, and RA. Previous text was often more implicit than explicit.

		Clarified text throughout the document that referred to "the" CA; text now refers to "a CA," which applies to both the PCA and ICAs. Changed many requirements of Relying Parties from MUST or SHALL to SHOULD since the PA cannot mandate that Relying Parties meet such requirements. Other editorial changes to remove ambiguity and improve clarity. Section 6.1.5: Changed CSS Certificate and End-Entity Authentication Certificate key sizes from 3072 to 2048 per NENA-STA-010.3b-2021 section 5.5. Section 1.3 PKI Participants added ICA Policy Authority and Agency Representatives, and removed the reference to NENA as Agency for the PCA. Section 1.4.2 changed MUST not use to SHALL NOT use, and defined a recommended 60-day time period for the PA to update the CP when new prohibited Certificate uses are added. Section 2.2.1 corrected the locations of the listed publications and added which entity provides them. Section 3.1.6 clarified that the PA SHALL attempt to resolve disputes involving names and trademarks, not the CA or RA. In the Foreward, Section 3.2.6, and Section 9.1, removed reference to expectation that cross signing with the Federal Bridge will be pursued.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

		Section 4.4.3 clarified how a CA SHALL notify PKI Participants whenever it issues a CA Certificate.
V1.2	2024-03-15	Adds Eonti editorial edits, DigiCert CP review edits, DoD mapping to FBPKI CP edits and Signing Certificate use case.
V1.2	2024-06-26	Scrubbing of CP

TABLE OF CONTENTS

FOREWORD	19
1. INTRODUCTION	21
1.1 Overview	21
1.2 Document Name and Identification	23
1.2.1 Certificate Policy Name	23
1.2.2 Object Identifier (OID)	23
1.3 PKI Participants	24
1.3.1 Policy Authority (PA)	24
1.3.2 Management Authority (MA)	25
1.3.3 Certification Authority (CA)	25
1.3.4 Registration Authority (RA)	26
1.3.5 Subscribers	26
1.3.6 Relying Parties	27
1.3.7 Other Participants	27
1.3.7.1 ICA Policy Authority	27
1.3.7.2 Agency	27
1.3.7.3 Agency Representative	27
1.3.7.4 PKI Sponsor	27
1.3.7.5 Compliance Auditor	28
1.4 Certificate Usage	28
1.4.1 Appropriate Certificate Uses	28
1.4.2 Prohibited Certificate Uses	29
1.5 Policy Administration	29
1.5.1 Organization Administering the Document	29
1.5.2 Contact Person	29
1.5.3 Person Determining CPS Suitability for this CP	30
1.5.4 CPS Approval Procedures	30
1.6 Definitions, Acronyms	30
1.7 References	30

2.	PUBLICATION AND REPOSITORY RESPONSIBILITIES	31
2.1	Repositories	31
2.2	Publication of Certification Information	31
2.2.1	Publication of CA Information	31
2.2.2	Availability of Information	32
2.3	Time or Frequency of Publication	32
2.4	Access Controls on Repositories	32
2.4.1	Certificate Policy	32
2.4.2	Certificates and CRLs	32
3.	IDENTIFICATION AND AUTHENTICATION	33
3.1	Naming.....	33
3.1.1	Types of Names.....	33
3.1.2	Need for Names to be Meaningful.....	34
3.1.3	Anonymity or Pseudonymity of Subscribers	34
3.1.4	Rules for Interpreting Various Name Forms	34
3.1.5	Uniqueness of Names	34
3.1.6	Recognition, Authentication, and Role of Trademarks.....	34
3.2	Initial Identity Validation	35
3.2.1	Method to Prove Possession of Private Key	35
3.2.2	Authentication of Organization Identity	36
3.2.3	Authentication of Subscriber Identity	36
3.2.4	Non-verified Subscriber Information.....	36
3.2.5	Validation of Authority.....	36
3.2.6	Criteria for Interoperation	36
3.3	Identification and Authentication for Re-Key Requests	36
3.3.1	Identification and Authentication for Routine Re-Key.....	36
3.3.2	Identification and Authentication for Re-Key after Revocation.....	36
3.4	Identification and Authentication for Revocation Request	37
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	38
4.1	Certificate Application	38
4.1.1	Who Can Submit a Certificate Application	38

4.1.2	Enrollment Process and Responsibilities	38
4.2	Certificate Application Processing	38
4.2.1	Performing Identification and Authentication Functions	38
4.2.2	Approval or Rejection of Certificate Applications	38
4.2.3	Time to Process Certificate Applications	39
4.3	Certificate Issuance	39
4.3.1	CA Actions During Certificate Issuance	39
4.3.2	Notification to Subscriber by the CA of Issuance of Certificates	39
4.4	Certificate Acceptance	39
4.4.1	Conduct Constituting Certificate Acceptance	40
4.4.2	Publication of the Certificate by the CA	40
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	40
4.5	Key Pair and Certificate Usage	40
4.5.1	Subscriber Private Key and Certificate Usage	40
4.5.2	Relying Party Public Key and Certificate Usage	40
4.6	Certificate Renewal	41
4.6.1	Circumstances for Certificate Renewal	41
4.6.2	Who May Request Renewal	41
4.6.3	Processing Certificate Renewal Requests	41
4.6.4	Notification of Certificate Renewal to Subscriber	41
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate	41
4.6.6	Publication of the Renewal Certificate by the CA	41
4.6.7	Notification of Certificate Renewal by the CA to Other Entities	42
4.7	Certificate Re-Key	42
4.7.1	Circumstances for Certificate Re-Key	42
4.7.2	Who May Request Certification of a New Public Key (Re-Key)	42
4.7.3	Processing Certificate Re-Keying Requests	42
4.7.4	Notification of New Certificate Issuance to Subscribers	42
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate	42
4.7.6	Publication of the Re-Keyed Certificate by the CA	42
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	43

4.8	Certificate Modification	43
4.8.1	Circumstance for Certificate Modification	43
4.8.2	Who May Request Certificate Modification	43
4.8.3	Processing Certificate Modification Requests.....	43
4.8.4	Notification of Modified Certificate Issuance to Subscriber	44
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	44
4.8.6	Publication of the Modified Certificate by the CA	44
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	44
4.9	Certificate Revocation and Suspension	44
4.9.1	Circumstances for Revocation	44
4.9.2	Who Can Request Revocation	45
4.9.3	Procedure for Revocation Request	45
4.9.4	Revocation Request Grace Period	46
4.9.5	Time Within Which CA Must Process the Revocation Request	46
4.9.6	Revocation Checking Requirement for Relying Parties	46
4.9.7	CRL Issuance Frequency	47
4.9.8	Maximum Latency for CRLs	47
4.9.9	Online Revocation/Status Checking Availability	48
4.9.10	Online Revocation Checking Requirements	48
4.9.11	Other Forms of Revocation Advertisements Available	48
4.9.12	Special Requirements Regarding Key Compromise	48
4.9.13	Circumstances for Suspension	48
4.9.14	Who Can Request Suspension	48
4.9.15	Procedure for Suspension Request.....	48
4.9.16	Limits on Suspension Period	49
4.10	Certificate Status Services (CSS).....	49
4.10.1	Operational Characteristics	49
4.10.2	Service Availability	49
4.10.3	Operational Features.....	50
4.11	End of Subscription	50
4.12	Key Escrow and Recovery	50

4.12.1 Key Escrow and Recovery Policy and Practices.....	50
4.12.2 Session Key Encapsulation and Recovery Policy and Practices.....	50
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	51
5.1 Physical Controls.....	51
5.1.1 Site Location and Construction	51
5.1.2 Physical Access.....	51
5.1.2.1 Physical Access for CA Equipment	51
5.1.2.2 Physical Access for RA Equipment	52
5.1.3 Power and Air Conditioning	52
5.1.4 Water Exposures	52
5.1.5 Fire Prevention and Protection.....	52
5.1.6 Media Storage	52
5.1.7 Waste Disposal	53
5.1.8 Off-Site Backup	53
5.2 Procedural Controls	53
5.2.1 Trusted Roles	53
5.2.1.1 CA Administrator	54
5.2.1.2 CA Operations Staff	55
5.2.1.3 Security Auditor	55
5.2.1.4 RA Staff	55
5.2.2 Number of Persons Required per Task	56
5.2.3 Identification and Authentication for Each Role.....	56
5.2.4 Roles Requiring Separation of Duties	57
5.3 Personnel Controls.....	57
5.3.1 Qualifications, Experience, and Clearance Requirements	57
5.3.2 Background Check Procedures.....	57
5.3.3 Training Requirements.....	58
5.3.4 Retraining Frequency and Requirements	58
5.3.5 Job Rotation Frequency and Sequence	58
5.3.6 Sanctions for Unauthorized Actions	59
5.3.7 Independent Contractor Requirements.....	59

5.3.8	Documentation Supplied to Personnel	59
5.4	Audit Logging Procedures.....	59
5.4.1	Types of Events Recorded	59
5.4.2	Requirements for Time-Stamping of Audit Records	62
5.4.3	Frequency of Processing Log	62
5.4.4	Retention Period for Audit Log.....	62
5.4.5	Protection of Audit Logs	62
5.4.6	Audit Log Backup Procedures	62
5.4.7	Audit Collection System (Internal vs. External)	62
5.4.8	Notification to Event-Causing Subject.....	63
5.4.9	Procedures to Obtain and Verify Audit Log Information	63
5.4.10	Vulnerability Assessments	63
5.5	Records Archival (Retention)	63
5.5.1	Types of Records Archived	63
5.5.2	Retention Period for Archive	64
5.5.3	Protection of Archive.....	64
5.5.4	Archive Backup Procedures	65
5.5.5	Requirements for Time-Stamping of Records.....	65
5.5.6	Archive Collection System (Internal or External)	65
5.5.7	Procedures to Obtain and Verify Archive Information	65
5.6	Key Changeover	65
5.7	Compromise and Disaster Recovery	66
5.7.1	Incident and Compromise Handling Procedures	66
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	66
5.7.3	Entity (CA) Private Key Compromise Procedures	67
5.7.3.1	PCA Compromise Procedures	67
5.7.3.2	Intermediate CA Compromise Procedures	68
5.7.3.3	CSS Compromise Procedures	68
5.7.3.4	RA Compromise Procedures	68
5.7.4	Business Continuity Capabilities after a Disaster.....	68
5.8	CA or RA Termination	69

6.	TECHNICAL SECURITY CONTROLS.....	70
6.1	Key Pair Generation and Installation	70
6.1.1	Key Pair Generation	70
6.1.1.1	CA Key Pair Generation	70
6.1.1.2	Subscriber Key Pair Generation	70
6.1.1.3	CSS Key Pair Generation	70
6.1.2	Private Key Delivery to Subscribers	70
6.1.3	Public Key Delivery to Certificate Issuer	71
6.1.4	CA Public Key Delivery to Relying Parties.....	71
6.1.5	Key Sizes	71
6.1.6	Public Key Parameters Generation and Quality Checking	71
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	71
6.1.7.1	<i>keyUsage</i> Extension for CA Certificates	72
6.1.7.2	<i>keyUsage</i> Extension for all End-Entity Certificates	72
6.2	Private Key Protection and Cryptographic Module Engineering Controls	73
6.2.1	Cryptographic Module Standards and Controls.....	73
6.2.2	Private Key (n out of m) Multi-Person Control.....	73
6.2.3	Private Key Escrow	74
6.2.4	Private Key Backup	74
6.2.4.1	Backup of CA Private Keys	74
6.2.4.2	Backup of Subscriber Private Keys	74
6.2.5	Private Key Archival	74
6.2.6	Private Key Transfer into or from a Cryptographic Module	74
6.2.7	Private Key Storage on Cryptographic Module.....	74
6.2.8	Method of Activating Private Key	74
6.2.8.1	CA Administrator Activation	75
6.2.8.2	Offline CAs Private Key	75
6.2.8.3	Online CAs Private Keys	75
6.2.9	Method of Deactivating Private Key.....	75
6.2.10	Method of Destroying Private Key	75
6.2.11	Cryptographic Module Rating.....	76

6.3	Other Aspects of Key Pair Management	76
6.3.1	Public Key Archival.....	76
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	76
6.4	Activation Data	77
6.4.1	Activation Data Generation and Installation	77
6.4.2	Activation Data Protection	77
6.4.3	Other Aspects of Activation Data	78
6.5	Computer Security Controls.....	78
6.5.1	Specific Computer Security Technical Requirements.....	78
6.5.2	Computer Security Rating.....	79
6.6	Life Cycle Technical Controls	79
6.6.1	System Development Controls	79
6.6.2	Security Management Controls	79
6.6.3	Life Cycle Security Controls	80
6.7	Network Security Controls.....	80
6.7.1	Isolation of Networked Systems.....	80
6.7.2	Boundary Protection	81
6.7.2.1	Transmission Confidentiality	81
6.7.3	Network Monitoring	81
6.8	Time-Stamping.....	81
7.	CERTIFICATE, CRL, AND OCSP PROFILES.....	82
7.1	Certificate Profile	82
7.1.1	Certificate Version Number(s).....	82
7.1.2	Certificate Extensions.....	82
7.1.2.1	Standard Extension for PCA Certificates	83
7.1.2.2	Standard Extension for ICA Certificates	83
7.1.2.3	Standard Extensions for End-Entity Certificates	84
7.1.2.4	Authority Information Access Extension	84
7.1.2.5	Authority Key Identifier Extension	85
7.1.2.6	Basic Constraints Extension	86
7.1.2.7	Certificate Policies Extension	87

7.1.2.8	CRL Distribution Points Extension	88
7.1.2.9	Extended Key Usage Extension	88
7.1.2.10	Key Usage Extension	89
7.1.2.11	Subject Alternative Name Extension	89
7.1.2.12	Subject Information Access Extension	92
7.1.2.13	Subject Key Identifier Extension	92
7.1.3	Algorithm Object Identifiers (OIDs)	93
7.1.4	Name Forms	94
7.1.4.1	PCA	94
7.1.4.2	ICAs	95
7.1.4.3	End-Entity Certificates	95
7.1.5	Name Constraints	96
7.1.6	Certificate Policy Object Identifier	96
7.1.7	Usage of Policy Constraints Extension	96
7.1.8	Policy Qualifiers Syntax and Semantics	96
7.1.9	Processing Semantics for the Critical Certificate Policies Extension	97
7.2	CRL Profile	97
7.2.1	CRL Version Number(s)	97
7.2.2	CRL and CRL Entry Extensions	97
7.3	OCSP Profile	98
7.3.1	OCSP Version Number(s)	98
7.3.2	OCSP Extensions	98
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	99
8.1	Frequency or Circumstances of Assessment	99
8.2	Identity and Qualifications of Assessor	99
8.3	Assessor's Relationship to Assessed Entity	99
8.4	Topics Covered by Assessment	99
8.5	Actions Taken as a Result of Deficiency	99
8.6	Communication of Results	100
8.7	Internal Audits	100

9.	OTHER BUSINESS AND LEGAL MATTERS	101
9.1	Fees	101
9.1.1	Certificate Issuance or Renewal Fees	101
9.1.2	Certificate Access Fees	101
9.1.3	Revocation or Status Information Access Fees	101
9.1.4	Fees for other Services.....	101
9.1.5	Refund Policy	101
9.2	Financial Responsibility	101
9.2.1	Insurance Coverage.....	101
9.2.2	Other Assets.....	101
9.2.3	Insurance or Warranty Coverage for End-Entities.....	101
9.3	Confidentiality of Business Information.....	102
9.3.1	Scope of Confidential Information.....	102
9.3.2	Information Not Within the Scope of Confidential Information	102
9.3.3	Responsibility to Protect Confidential Information	102
9.4	Privacy of Personal Information.....	102
9.4.1	Privacy Plan.....	102
9.4.2	Information Treated as Private	102
9.4.3	Information Not Deemed Private	103
9.4.4	Responsibility to Protect Private Information	103
9.4.5	Notice and Consent to Use Private Information.....	103
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	103
9.4.7	Other Information Disclosure Circumstances	103
9.5	Intellectual Property Rights	103
9.6	Representations and Warranties	104
9.6.1	CA Representations and Warranties	104
9.6.2	RA Representations and Warranties	104
9.6.3	Subscriber Representations and Warranties.....	105
9.6.4	Relying Parties Representations and Warranties.....	105
9.6.5	Representations and Warranties of Other Participants.....	105
9.7	Disclaimers of Warranties.....	105

9.8	Limitations of Liability	106
9.9	Indemnities.....	106
9.10	Term and Termination	106
9.10.1	Term.....	106
9.10.2	Termination.....	106
9.10.3	Effect of Termination and Survival	106
9.11	Individual Notices and Communications with PKI Participants	106
9.12	Amendments	106
9.12.1	Procedure for Amendment.....	106
9.12.2	Notification Mechanism and Period.....	106
9.12.3	Circumstances Under Which OID Must be Changed.....	107
9.13	Dispute Resolution Provisions	107
9.14	Governing Law	107
9.15	Compliance with Applicable Law	107
9.16	Miscellaneous Provisions	107
9.16.1	Entire Agreement.....	107
9.16.2	Assignment	107
9.16.3	Severability	107
9.16.4	Enforcement (Attorneys' Fees and Waiver of Rights)	107
9.16.5	Force Majeure	107
9.17	Other Provisions	107
APPENDICES		104
APPENDIX A - ABBREVIATIONS AND ACRONYMS.....		108
APPENDIX B - GLOSSARY		109
APPENDIX C - REFERENCES.....		116
TABLE OF TABLES		
TABLE 1: PUBLICATION REQUIREMENTS		31
TABLE 2: CERTIFICATE NAMES.....		33
TABLE 3: CRL ISSUANCE FREQUENCY.....		47
TABLE 4: AUDITABLE EVENTS RECORDED		60
TABLE 5: RECORDS RETENTION		63

TABLE 6: KEY PAIR GENERATION	70
TABLE 7: KEY SIZES.....	71
TABLE 8: <i>KEYUSAGE</i> EXTENSION FOR ALL CA CERTIFICATES	72
TABLE 9: <i>KEYUSAGE</i> EXTENSION FOR ALL AGENCY AND AGENT CERTIFICATES	72
TABLE 10: <i>KEYUSAGE</i> EXTENSION FOR ALL ELEMENT CERTIFICATES	73
TABLE 11: <i>KEYUSAGE</i> EXTENSION FOR ALL SIGNING CERTIFICATES	73
TABLE 12: CERTIFICATE VALIDITY PERIODS	76
TABLE 13: CERTIFICATE PROFILE BASIC FIELDS.....	82
TABLE 14: PCA CERTIFICATE STANDARD EXTENSIONS	83
TABLE 15: ICA CERTIFICATE STANDARD EXTENSIONS.....	83
TABLE 16: END-ENTITY CERTIFICATE STANDARD EXTENSIONS	84
TABLE 17: <i>AUTHORITYINFORMATIONACCESS</i> EXTENSION FOR ICA CERTIFICATES...	85
TABLE 18: <i>AUTHORITYINFORMATIONACCESS</i> EXTENSION FOR END-ENTITY CERTIFICATES.....	85
TABLE 19: <i>AUTHORITYKEYIDENTIFIER</i> EXTENSION FOR ICA CERTIFICATES	86
TABLE 20: <i>AUTHORITYKEYIDENTIFIER</i> EXTENSION FOR END-ENTITY CERTIFICATES	86
TABLE 21: <i>BASICCONSTRAINTS</i> EXTENSION FOR ROOT CA CERTIFICATES	87
TABLE 22: <i>BASICCONSTRAINTS</i> EXTENSION FOR TIER-2 ICA CERTIFICATES	87
TABLE 23: <i>BASICCONSTRAINTS</i> EXTENSION FOR TIER-N ICA CERTIFICATES	87
TABLE 24: <i>CRLDISTRIBUTIONPOINTS</i> EXTENSION FOR ICA CERTIFICATES.....	88
TABLE 25: <i>CRLDISTRIBUTIONPOINTS</i> EXTENSION FOR END-ENTITY CERTIFICATES	88
TABLE 26: <i>EXTENDEDKEYUSAGE</i> EXTENSION FOR ELEMENT CERTIFICATES	89
TABLE 27: <i>EXTENDEDKEYUSAGE</i> EXTENSION FOR SIGNING CERTIFICATES	89
TABLE 28: <i>SUBJECTALTERNATIVEName</i> EXTENSION FOR ROOT CERTIFICATES	91
TABLE 29: <i>SUBJECTALTERNATIVEName</i> EXTENSION FOR ICA CERTIFICATES.....	91
TABLE 30: <i>SUBJECTALTERNATIVEName</i> EXTENSION FOR END-ENTITY CERTIFICATES	92
TABLE 31: <i>SUBJECTINFORMATIONACCESS</i> EXTENSION FOR ICA CERTIFICATES.....	92
TABLE 32: <i>SUBJECTKEYIDENTIFIER</i> EXTENSION FOR CA CERTIFICATES.....	93
TABLE 33: <i>SUBJECTKEYIDENTIFIER</i> EXTENSION FOR END-ENTITY CERTIFICATES	93
TABLE 34: PCA CERTIFICATE SUBJECT FIELDS	94
TABLE 35: ICA CERTIFICATE SUBJECT FIELDS	95

TABLE 36: END-ENTITY CERTIFICATE SUBJECT FIELDS.....	95
TABLE 37: <i>CERTIFICATEPOLICIES</i> EXTENSION FOR ICA CERTIFICATES	96
TABLE 38: <i>CERTIFICATEPOLICIES</i> EXTENSION FOR END-ENTITY CERTIFICATES.....	96
TABLE 39: CRL PROFILE BASIC FIELDS.....	97
TABLE OF FIGURES	
FIGURE 1: PCA PKI ARCHITECTURE.....	22

Foreword

Background

Certification Authorities (CAs), and the infrastructure they support, form the basis for one of the primary mechanisms for providing assurance of identity. The widely placed trust in CAs is at the heart of security mechanisms used to protect sessions and transactions for Next Generation 9-1-1 (NG9-1-1). National Emergency Number Association's i3 [NENA i3] and associated standards require Transport Layer Security (TLS) throughout the ecosystem to allow for secure communications and a single shared root of trust to assist with interoperability. TLS relies on CAs to identify servers and clients. The root of trust in the NG9-1-1 Public Key Infrastructure (PKI) is the Public Safety Answering Point (PSAP) Credentialing Agency (PCA).

The purpose of this document is to provide security requirements needed to support the secure issuance of Certificates¹ in NG9-1-1 by the PCA CAs in the NG9-1-1 PKI. In particular, this document has been developed to provide an appropriate level of assurance to support government emergency services including public safety, and applications, i.e., a high level of assurance as defined in the Validation Policy (VP). The level of assurance refers to the strength of the Binding between the Public Key and the entity whose name is cited in the Certificate, the policies used to control the use of the corresponding Private Key, and the overall security provided by the PKI itself.

The PCA is a functional element in the NENA i3 Standard for Next Generation 9-1-1 core services² which establishes a root of trust for the NG9-1-1 ecosystem to facilitate interoperable security between disparate NG9-1-1 environments. The NENA i3 standard includes not only a shared root of trust to build a PKI, but it also standardizes how identities are conveyed across NG9-1-1, and what roles those identities have in the NG9-1-1 ecosystem. In addition to participating within a PKI in a trusted environment, the standardization of conveying identities and roles provides for powerful abilities to manage permissions and other security configurations in NG9-1-1 that work across different NG9-1-1 environments and disparate public safety systems. The PCA as set forth in this document supports all of the functionality as required by the NENA i3 standard to provide a PCA.

Certificate Policy

This baseline set of requirements has been written in the form of a "Certificate Policy." The International Telecommunication Union (ITU) Recommendation X.509, defines a "Certificate Policy" as "a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements." That is, a Certificate Policy (CP) defines the expectations and requirements of the PKI Participants (e.g., Subscribers, Relying Parties, etc.) that will

¹ Capitalized words in this document are defined terms in the glossary – Appendix B.

² See NENA STA-010.3x. Available at <https://www.nena.org/page/Standards>.

trust the Certificates issued by its CAs. This document is also written to fulfill requirements set forth in [NENA i3](#), fulfilling the PSAP Credential Agency (PCA) functional element.

The governance structure that represents the PKI Participants is known as the Policy Authority (PA). The NG9-1-1 Interoperability Oversight Commission (NIOC) created by NENA is the PA for the PCA. The PA is responsible for identifying the appropriate set of requirements for a given community and oversees the CAs that issue Certificates for that community. This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework [[RFC 3647](#)]. The United States Government's Federal PKI Common Policy (FPKI Common Policy) [[FPKIPA](#)] was used as a base document for this CP. The FPKI Common Policy is widely recognized for clearly articulating the requirements for Certificate issuance for the Certificates, which are primarily used by government entities to Authenticate to government systems.

1. Introduction

The traditional analog voice-centric 9-1-1 system is no longer able to support many of the common communication methods in use today. NENA and other standards bodies have developed a NG9-1-1 system that modernizes emergency calling systems by allowing multiple forms of multimedia communications, native location handling, and enhanced routing mechanisms. To enable secure communication between Relying Parties, a PSAP Credentialing Agency (PCA) PKI has been created. This CP sets the requirements for the use of PKI Certificates for NG9-1-1 and follows the technical requirements set forth in the NENA i3 Standard for NG9-1-1 [[NENA i3](#)].

1.1 Overview

A Certification Authority (CA) is a collection of hardware, software, personnel, and operating procedures that issue and manage Public Key Certificates, also known as digital Certificates. The Certificate binds the Certificate holder's (also known as the Subscriber) Public Key to a set of named Subject attributes identifying the Subscriber. This allows Relying Parties to Authenticate and trust signatures or assertions made by the Subject contained in the Certificate.

A fundamental element of modern secure communications is establishing trust in Public Keys via Public Key Certificates. This begins with a Relying Party obtaining an entity's Public Key Certificate that is issued by a trusted entity (e.g., a Trust Anchor) certifying that the Public Key belongs to that entity as the Subscriber of the Certificate. Entities that are not trusted directly MAY become trusted through successive validation of their Subscriber Certificate through a hierarchical chain of CA Certificates from the Subscriber's Certificate to a Trust Anchor (typically a Root CA (hereafter the PCA) Public Key). Trust Anchors are an authoritative entity for which trust is assumed and not derived and thus are explicitly trusted by Relying Parties. Relying Parties SHALL be responsible for securely obtaining Trust Anchors (e.g., the PCA Public Key) and for securely managing their Trust Anchor store (e.g., a database containing a set of CAs used as Trust Anchors). Relying Parties MUST configure Trust Anchors in their Trust Anchor stores with great caution and MUST give full consideration to the requirements of this CP and [NENA i3](#).

A Certificate issued in accordance with this CP conveys within the NG9-1-1 community a level of digital identity proofing associated with the Subject of the Certificate and membership within the NG9-1-1 PKI. Certificates within the NG9-1-1 PKI communicate three (3) important things within the NG9-1-1 ecosystem to allow for security and interoperability: an entity's Agency, and entity's identity and the entity's role within NG9-1-1 (for example, as a first responder with a specific role, a call taker or as a functional element within NG9-1-1 core services). These values are included in the Certificate Subject Alternative Name (SAN).³

³ See NENA STA-010.3-2020 at Section 6: Security.

Other important documents supporting this CP in the PCA PKI include the CA Certification Practice Statement(s) (CPSs) and Subscriber agreements.

The PCA PKI shown in Figure 1 is comprised of a mandatory offline PCA at tier 1, an Intermediate CA (ICA) at tier 2, and End-Entity Certificates at the bottom tier. Branches of the PKI MAY include several more tiers per Section 7.1.2.6 of this CP.

Note: Tier 2 can be expanded to add multiple optional ICA Tiers below it, by approval of the NIOC, to support current and future use cases for the PCA, as the need for digital Certificates evolves in the deployment of the PKI. Current use cases involve creating generic Hosted ICAs so that any integrator can receive their Certificates directly from the Hosted ICA, or to create ICAs dedicated to a specific integrator to meet their Certificate issuance requirements. Tier 2 is also where ICA cross-certification can take place and also where resigning of third party ICAs with the PCA can occur, as long as the third party ICAs are compliant with this CP and its cross-certification requirements. For future use cases, the PKI could add ICAs for issuance of Agent and Signing Certificates. The PKI is designed to be flexible to meet the varying needs of the NG9-1-1 community.

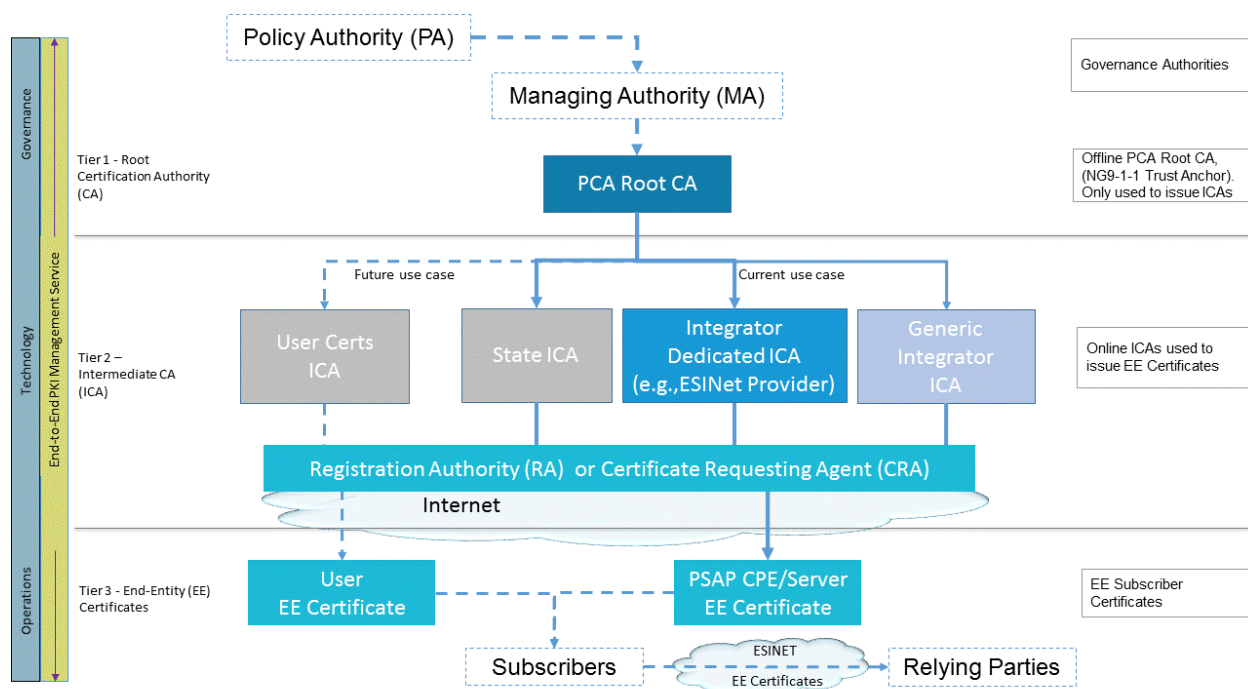


Figure 1: PCA PKI Architecture

Throughout this CP, the words that are used to define the significance of particular requirements are capitalized. These words are defined in [RFC 2119](#).

These words are:

"MUST"	This word, or the terms "REQUIRED" OR "SHALL", means that the definition is an absolute requirement of the specification.

"MUST NOT"	This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
"SHOULD"	This word, or the adjective "RECOMMENDED", means that there MAY exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase, or the phrase "NOT RECOMMENDED", means that there MAY exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word, or the adjective "OPTIONAL", means that an item is truly optional. One Subscriber MAY choose to include the item because a particular marketplace requires it, or because the Subscriber enhances the product, while another Subscriber MAY omit the same item.

This CP uses tables in Section 6: Technical Security Controls, and Section 7: Certificate, CRL, and OCSP Profiles. In order to make these tables easier to follow, they are color coded as follows:

	General tables (applying to this CP or to all Certificates)
	PCA
	ICAs
	All CAs
	End-Entity Certificates
	Certificate Status Service (OCSP and CRL)

This CP uses the following naming convention of *lowerCamelCase*, for x509 extensions and attributes.

1.2 Document Name and Identification

1.2.1 Certificate Policy Name

This document is the PCA PKI Certificate Policy and has been approved for publication by the NIOC.

1.2.2 Object Identifier (OID)

Certificates issued by the PCA under this CP SHALL contain the PCA Object Identifier (OID), 1.3.6.1.4.1.55670.1. The OID SHALL be available to Relying Parties in each Certificate via the *certificatePolicies* extension.

NENA is requested to establish a Registry in the NENA Registry System (NRS) to maintain child OIDs under the PCA OID. The name of this sub-registry is "PCA Sub-registry". A new entry to the PCA Sub-registry SHALL be approved by NIOC in a written policy made available at <https://ng911ioc.org>. This policy SHALL include an explanation

of when the child OID will be used, and how its use distinguishes it from other child OIDs.

This registry SHALL include the following initial values:

Quad ID OID	Purpose	Reference
1.3.6.1.4.1.55670.1.1	Quad string for valid <i>otherName</i> values for the <i>subjectAlternativeName</i> extension required in all NG9-1-1 PKI Certificates.	This document

1.3 PKI Participants

This section identifies PCA PKI Participants that are relevant to the administration and operation of the PKI under this CP, including the:

- PCA Policy Authority (PA) - NIOC;
- ICA PA – Tier 2 (or lower) ICA operator PA approved by NIOC;
- Management Authority (MA) – NENA, delegated to Eonti;
- Certification Authority – DigiCert for the PCA;
- Registration Authority (RA) – Eonti for the PCA;
- Subscribers – PCA PKI Certificate holders (inclusive of both ICAs and End-Entity Certificate holders), for example, Agencies, Elements, and Agents;
- Relying Parties – NG9-1-1 community; and
- Agency Representatives – See the [VP](#).

1.3.1 Policy Authority (PA)

NENA, at the direction of its standards development community, including the NENA Development Steering Council, 9-1-1 Core Services Committee, and the NENA Executive Board, has established the NIOC, according to the bylaws of the NIOC.

The NIOC is the PA for the PCA PKI.

The PA is the owner of the PCA PKI and is responsible for setting up and approving policies and practices governing the PKI.

Responsibilities of the PA include:

- Establishing and approving this CP;
- Governing the PKI according to this CP;
- Approving the establishment of trust relationships with external PKIs;
- Approving the CPS for CAs that issue Certificates under this CP;
- Approving the Audits for CAs operating under this CP;
- Approving any revisions to this CP; and
- Performing MA activities listed below in the absence of a MA.

ICAs MAY employ an ICA PA to institute additional policies that apply to their ICA and any Certificates issued by that ICA, such as changes to the CPS for that ICA. The CPS

for an ICA that has a PA SHALL describe the authority, responsibilities and powers of that PA. Any policies adopted by the ICA PA SHALL conform with the CP. ICA PA policies MAY be more stringent than the CP, but SHALL NOT be less stringent than the CP. Unless stated otherwise, "PA" in the CP means NIOC.

1.3.2 Management Authority (MA)

The PA oversees the MA to provide trust management services to support the NG9-1-1 ecosystem in meeting its security goals in using the PCA PKI. The PA MAY perform the MA duties itself or designate a trusted third party to act as the MA on its behalf to provide operational support and maintain the PKI in accordance with this CP. The PA has designated NENA to be the MA for the PCA PKI. While NENA retains overall responsibility for the PCA to ensure the responsibilities of the MA are fulfilled, day-to-day function of the MA is delegated to Eontic Inc. (Eontic). For any ICA (i.e., Hosted or Discrete), the MA is designated in the CPS for the ICA.

The MA's primary focus is to ensure that policies for secure physical and logical Access, data sharing, and communications across the ecosystem are realized through the execution and management of the CP requirements and its participants. The MA is responsible for the following:

- The Process for CAs to submit CPSs;
- Approval of the process for recognizing Prospective Subscribers, their authorized representatives, and their agreements;
- Ensuring continued conformance of each CA that issues Certificates under this CP with applicable requirements as a condition for allowing continued participation;
- Approval of the process for Revocation requests;
- Approval of the process for Audits; and
- Approval of the process to approve Subscriber authorizations.

1.3.3 Certification Authority (CA)

The CA is the collection of hardware, software and operating personnel that create, sign, and issue Public Key Certificates to Subscribers. Within this CP, the acronym "CA or CAs" includes the Root and ICAs. If a requirement only applies to the PCA, it will denote PCA. If it only applies to ICAs hosted by DigiCert, it will denote Hosted ICA. If it only applies to ICAs operated by the Subscriber or a third party on behalf of the Subscriber, it will be denoted as a Discrete ICA.

The CA is responsible for:

- Approving the issuance of all Certificates it issues, including those issued to next tier ICAs;
- Revoking Certificates;
- Providing the PA, MA, and RA with CA Certificates it has issued;
- Generating, protecting, operating, and destroying its CA Private Keys;
- Establishing and maintaining its CPS;

- Certificate Status Service (CSS) including Online Certificate Status Protocol (OCSP) responder and Certificate Revocation List (CRL) generation and distribution;
- Repository management of Certificate related items;
- Managing all aspects of the CA services, operations and infrastructure related to Certificates (e.g., security Audit, configuration management, and Archive);
- Onboarding Prospective Subscribers to the Certificate issuance process; and
- Securing delivery of Certificates to its Subscriber.

DigiCert, Inc. (DigiCert) operates the PCA and any Hosted ICAs under contract to NENA, at the direction of NIOC. Stand-alone ICAs MAY be hosted by the Subscriber or by a third party on behalf of the Subscriber with a signed ICA Certificate from the PCA or the appropriate upper-level ICA. The first tier MUST be approved by NIOC. All other ICAs in the NG9-1-1 PKI MUST also conform with this CP and develop a CPS approved by the appropriate PA for that CA, regardless of operator.

1.3.4 Registration Authority (RA)

The RA is an authority that performs Certificate management functions on behalf the CA, such as collection and verification of a Prospective Subscriber's identity and information that is to be entered into the Subscriber's Public Key Certificate. The RA performs its function in accordance with this CP, as well as any additional relevant policies and procedures included in the CA's CPS. Eonti is the RA for the Hosted ICAs. Discrete ICAs MAY employ an RA to assist the CA in its Certificate management functions. In this document, if a requirement only applies to the CA, it will denote CA. If it applies to the RA on behalf of the CA, it will denote RA.

The RA is responsible for:

- Control over the account registration process;
- Verifying the identity of the Prospective Subscriber for their respective ICA;
- Onboarding Prospective Subscribers to the Certificate issuance process, converting them to a Subscriber;
- Requesting Certificates on behalf of the Subscriber; and
- Delivery of End-Entity Certificates to the Subscriber.

1.3.5 Subscribers

A Subscriber is the entity whose name appears as the Subject in an End-Entity Certificate (also known as a Subscriber Certificate), who agrees to use its Private Key and Certificate in accordance with the Certificate Policy asserted in the Certificate, and that does not itself issue Certificates.

Subscribers are responsible for:

- Executing the applicable Subscriber agreement (i.e., the Digital Certificate Subscriber Agreement (DCSA));
- Completing the requested Certificate Application information;
- Responding to verification requests in a timely manner;

- Generating the asymmetric Key Pair and protecting their Private Key;
- Delivering the Public Key of the Key Pair to the RA as part of their Certificate request; and
- Using the Certificate and corresponding Private Key in compliance with this CP.

CAs are sometimes technically considered “Subscribers” in a PKI. However, the term “Subscriber” as used in this document refers only to those who request Certificates for uses other than signing and issuing Certificates or Certificate status information.

1.3.6 Relying Parties

A Relying Party is an entity that relies on the validity of the Binding of the Subscriber’s name to a Public Key. The Relying Party uses a Subscriber’s Certificate to verify or establish the identity and status of the Subscriber. A Relying Party is responsible for deciding whether or how to check the validity of the Certificate by checking the appropriate Certificate status information. A Relying Party MAY use information in the Certificate to determine the suitability of the Certificate for a particular use.

1.3.7 Other Participants

The PCA PKI MAY require the services of other security, community, and application authorities. If required, the appropriate PA SHALL identify the parties, define the services, and designate the mechanisms used to support these services.

1.3.7.1 ICA Policy Authority

An ICA MUST have a corresponding PA, which is referred to as an ICA PA. The NIOC can be the PA for an ICA that does not have its own PA.

1.3.7.2 Agency

An Agency is a Public Safety Entity⁴ that is eligible to hold an Agency Certificate.⁵ The PCA’s RA MUST Authenticate the Agency according to the [VP](#). The Agency MAY then designate an Agency Representative to act on its behalf, to authorize PKI Sponsors or for other purposes outlined in future versions of this CP.

1.3.7.3 Agency Representative

An Agency Representative is an authorized representative for an Agency.

1.3.7.4 PKI Sponsor

A PKI Sponsor is an individual who is to be explicitly responsible for managing Access to the Private Key associated with a device Certificate when the Subscriber is a device. The Agency or its Agency Representative SHALL authorize the PKI Sponsor and MAY provide identifying information for the device during the Certificate request for the device.

⁴ See [VP](#) Section 3.7.

⁵ See [VP](#) Section 3.2.

1.3.7.5 Compliance Auditor

The Compliance Auditor is an individual or entity who is responsible for Auditing the security of CAs, including reviewing, maintaining, and Archiving Audit logs; and performing or overseeing Audits of CAs. The Compliance Auditor MUST have expertise in information security, cryptography, and PKI, Risk mitigation strategies, and industry best practices. A single individual MAY perform the Audit, but MUST NOT be affiliated with the entity being Audited. The CA SHALL identify in the CPS the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued under this CP represent a high level of assurance⁶, as defined in the [VP](#), which is relevant to environments where Risks and consequences of identity and data Compromise are severe.

Two (2) types of End-Entity Certificates are issued to Subscribers conforming to this CP; Authentication Certificates (e.g., Element, Agency and Agent Certificates) and Signing Certificates. Certificates SHOULD be issued in pairs, one (1) Authentication and one (1) Signing Certificate with the same Certificate Validity Period, Distinguished Name (DN) and Subject Alternative Name.

Certificates issued within the NG9-1-1 PKI are to be used for Authentication and signing purposes, as designated by the *keyUsage* and *extKeyUsage* fields found within the Certificate, for entities connected to an Emergency Services IP Network (ESInet) to protect services for, or ancillary to, public safety or processing emergency calls.

Specifically, applicable Certificate uses include:

- PCA issuance of ICA Certificates, CSS Certificates, and CRLs;
- ICA, which are CAs subordinate to the PCA, issuance of ICA CRLs. ICAs MAY issue other ICA Certificates and Subscriber End-Entity Certificates, as well as local CSS Certificates;
- CSSs sign OSCP responses; and
- End-Entity Certificates are used for purposes described in NENA-STA-010.3-2020 and other applicable NENA Standards as determined by NIOC.
 - o Authentication Certificates issued by the PCA are to be used for Authentication purposes, *as designated* by the *keyUsage* and *extKeyUsage* fields found within the Certificate, for entities connected to an ESInet to protect services for, or ancillary to, public safety or processing emergency calls.
 - o Signing Certificates issued by the PCA are to be used for signing purposes, as designated by the *keyUsage* and *extKeyUsage* fields found within the

⁶ Commensurate with NIST SP-800-63 [SP 800-63] series Identity Assurance Level 3.

Certificate, for entities connected to an ESInet to protect services for, or ancillary to, public safety or processing emergency calls.

The PA MAY allow additional permitted uses not included in this CP by an affirmative vote of its members in accordance with its bylaws. In such cases, the PA SHOULD update this CP with those permitted activities within a reasonable period of time.

1.4.2 Prohibited Certificate Uses

Certificates issued by the PCA are generally not appropriate for use in commercial transactions. In limited cases, they MAY be used in commercial transactions related to public safety. Other prohibited applications include:

- Any export, import, use, or activity that contravenes any local or international laws or regulations;
- Any usage of Certificates in conjunction with illegal activities;
- Any usage of Certificates for personal use or purposes not related to the community's operation;
- Any use of a Certificate after it has been Revoked;
- Any use of a Certificate after it has expired; and
- Any use not expressly permitted in Section 1.4.1.

Additionally, Subscribers and Relying Parties SHALL NOT use, Certificates issued by the PCA for Authentication outside of communications directly related to NG9-1-1, unless expressly permitted by the PA. The PA MAY add prohibited uses not included in this CP by an affirmative vote of its members in accordance with its bylaws. In such cases, the PA SHOULD update this CP with those prohibited activities no later than sixty (60) days from the date of the affirmative vote.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is administered by the NIOC as the PA. It owns this CP and represents the interest of its members in developing the policies that govern the PCA PKI. Additional policies or exceptions to these policies enacted by the PA under an affirmative vote of its members in accordance with its own bylaws and updating this CP with these changes within a reasonable period of time.

1.5.2 Contact Person

The following individual is responsible for accepting comments on this CP on behalf of NIOC:

NG9-1-1 Interoperability Oversight Commission
c/o NENA
Director of Technology
1700 Diagonal Blvd
Suite 1700
Alexandria, VA 22314

admin@ng911ioc.org

+1 202 466 4911

1.5.3 Person Determining CPS Suitability for this CP

The PCA PA SHALL approve the CPS for the PCA and all lower-tier ICAs.

1.5.4 CPS Approval Procedures

CAs SHALL submit their CPS to the appropriate MA. The MA SHALL evaluate CAs against all facets of this CP.

The appropriate PA SHALL approve the CPS if it determines that the CPS complies with this CP. The CA MUST meet all requirements of an approved CPS before commencing operations.

1.6 Definitions, Acronyms

See Appendices Appendix A and Appendix B.

1.7 References

See Appendix C.

2. Publication and Repository Responsibilities

2.1 Repositories

All CAs that issue Certificates under this CP MUST post all CRLs issued by the CA in a Repository that is Accessible through Uniform Resource Identifier (URI) references asserted in valid Certificates issued by that CA. The PKI Repositories containing Certificates and Certificate status information SHALL be deployed so as to provide high levels of availability as appropriate for the entity's environment and service level agreement. This service level agreement MUST be included in every CPS. To promote consistent Access to Certificates and CRLs, the Repository SHALL implement Access Controls and communication mechanisms to prevent unauthorized Modification or deletion of information.

CAs SHALL provide their CA Certificate and any CA Certificates they have issued in a Repository that is available to the PKI Participants.

2.2 Publication of Certification Information

2.2.1 Publication of CA Information

The PA SHALL make the CP publicly available, and the CA SHALL make CRLs, and CA Certificates available as shown on Table 1. In general, the CPS for CAs is confidential, but it SHALL be made available to participating members, in a redacted version, from the appropriate PA. The CA SHALL protect information not intended for public dissemination.

Table 1 below is a matrix of the various PKI practice documents, showing whether or not they are publicly available, and their locations. The list is not intended to be exhaustive, nor will each document listed be applicable to every CA. Documents not expressly made public are confidential to preserve the security of the PCA PKI.

Table 1: Publication Requirements

Item	Classification	Available From:	Available At:
PCA PKI CP	Public	PA	https://ng911ioc.org/library
Bylaws	Public	PA	https://ng911ioc.org/library
PCA Certificate	Public	PA	https://ng911ioc.org/library
ICA Certificates	Public	PA	https://ng911ioc.org/library
PCA CRLs	Public	CA	<CA Repository URI>
ICA CRLs	Public	CA	<CA Repository URI>

PCA CPS	Portions confidential	PA	https://ng911ioc.org/library (redacted version)
ICA CPS	Portions confidential	CA	<CA Repository URI> (redacted version)
Subscriber guides	Public	RA	<RA Repository URI>

2.2.2 Availability of Information

CAs SHALL make all information published in the Repository available on a twenty-four (24) hour per day, seven (7) day per week basis, save for periods of scheduled or unscheduled downtime, as negotiated between relevant parties as part of a commercial contract.

CAs SHALL retain all information in the Repository, including non-public information, specifically all End-Entity Certificates, for a period of three (3) years from the expiration of the information.

2.3 Time or Frequency of Publication

The PA SHALL make updated versions of this CP publicly available within ten (10) business days of the incorporation of changes.

CA Certificates SHALL be made publicly available within ten (10) business days after issuance.

CAs MUST publish CRLs as specified in Section 4.9.7.

All other information to be published in the Repository SHALL be published promptly after such information becomes available to the CA. The maximum time for publication of information SHALL be specified in the CPS.

2.4 Access Controls on Repositories

2.4.1 Certificate Policy

The PA SHALL make this CP publicly available as shown in Table 1 for read-only Access.

2.4.2 Certificates and CRLs

The CA SHALL protect information not intended for public dissemination or Modification. CA Certificates and CRLs in the Repository SHALL be publicly available for read-only Access through the Internet. The CPS SHALL detail what information in the Repository SHALL be exempt from automatic availability and to whom, and under what conditions the restricted information MAY be made available.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The CAs SHALL assign non-empty X.500 Distinguished Names (DNs) [X.500] to the issuer and *subjectDN* fields of the Certificates issued as shown in Table 2. CAs MAY create Subscriber Certificates that contain any name type appropriate to the application. The CA MUST assign DN in the form of a X.500 *printableString* to the issuer and *subjectDN* fields. If the CA cannot encode the string as a *printableString*, it MUST encode it as a UTF8String [RFC 5280].

Table 2: Certificate Names

Certificate	Issuer DN	Subject DN
PCA Certificate	c=<two-letter ISO 3166-1 country code> o=<Organization Name> ou=PCA-<serial number> cn=PCA Root	c=<two-letter ISO 3166-1 country code> o=<Organization Name> ou=PCA-<serial number> cn=PCA Root
ICA Certificate	c=<two-letter ISO 3166-1 country code> o=<Organization Name> ou=PCA-<serial number> cn=PCA Root	c=<two-letter ISO 3166-1 country code> o=<Organization Name> or <state, regional, local 9-1-1 defined> ou=ICA-<serial number> [st=<state, regional, local 9-1-1 defined>] [l=<state, regional, local 9-1-1 defined>] cn=<Name> ICA
End-Entity Certificate	c=<two-letter ISO 3166-1 country code> o=<Organization Name> or <state, regional, local 9-1-1 defined> ou=CA-<serial number> [st=<state, regional, local 9-1-1 defined>] [l=<state, regional, local 9-1-1 defined>] cn=<Name> ICA	c=<two-letter ISO 3166-1 country code> o=<Subscriber Organization Name> [l=<city, regional, local 9-1-1 defined>] [st=<state, regional, local 9-1-1 defined>] [ou=<Organization Unit Name>] cn=<iD from the Quad ID>

Note: in the table above, <serial number> SHALL be any number, even sequential, that makes the *subjectDN* unique when issuing another Root CA or ICA Certificate with a similar DN. The *subjectDN* in End-Entity Certificates will not be unique during the Rollover Period.

3.1.2 Need for Names to be Meaningful

The RA MUST ensure that names used in all PCA PKI Certificates represent an unambiguous identifier for the Subject and that the Subject contains the verified organization name of the PKI Sponsor responsible for the Certificate. The RA MUST use the verified organization name as the *organizationName* field in the DN of the issued Certificate.

Relying Parties SHOULD use the *subjectAltName* (SAN) extension, as defined in Section 7.1.2.11, to assert the identity and role of the entity (e.g., person, organization, device, or object). Relying Parties SHALL use the Subject DN to verify the organization the Certificate was issued to. Relying Parties SHOULD use the Issuer DN to verify the issuer of the Certificate.

The Organization Name, or the o= field, SHOULD be the display name of the Owner, such as "NG9-1-1 Interoperability Oversight Commission" or "State of Virginia".

The Organizational Unit, or the ou= field, SHOULD be descriptive, down to an instance, of what the entity issued a Certificate does. For example, "PCA-1" or "State of Virginia ECRF-01".

The Common Name, or the cn= field, SHOULD be a display name, such as "PCA" or "Fairfax County ICA" for the Root and ICA Certificates. The cn= in End-Entity Certificates SHOULD be the *iD* field from the Quad ID.

3.1.3 Anonymity or Pseudonymity of Subscribers

The PCA and its RA, and ICAs and their RAs, SHALL NOT issue Anonymous or Pseudonymous Certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting DN forms are specified in [X.500](#).

3.1.5 Uniqueness of Names

The PCA and ICAs SHALL ensure that NENA Quad ID values in the Subject Alternative Name (SAN) extension in the Certificates they issue are unique. Certificate Re-Key and/or Renewal does not violate the requirement for name uniqueness.

The *subjectDN* in CA Certificates is unique when Certificates are Re-Keyed due to the serial number used in the ou= field.

The *subjectDN* in End-Entity Certificates is always unique because the *commonName* is the *iD* from the Quad ID field.

3.1.6 Recognition, Authentication, and Role of Trademarks

The PCA and its RA, and ICAs and their RAs, SHALL NOT knowingly issue a Certificate including the name that a court of competent jurisdiction has determined infringes upon a third party's trademark. Prospective Subscribers SHALL NOT use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others.

A CA or RA SHALL NOT knowingly issue a Certificate including the name of any entity, such as a government agency, that a court of competent jurisdiction would determine that the Prospective Subscriber is not a legitimate agent of, such as through employment (for Certificates issued to individual identities) or ownership/responsibility to operate (for Certificates issued to devices or software).

A CA or RA is not required to determine whether a Prospective Subscriber has Intellectual Property Rights or otherwise has Legal Agency in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any Intellectual Property Rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark; and the PA, and any CA SHALL be entitled, without liability to any Prospective Subscriber, to reject or suspend any DCSA because of such dispute. The PA SHALL attempt to resolve disputes involving names and trademarks.

3.2 Initial Identity Validation

This section provides the requirements for the issuance of high assurance Certificates under this CP. The word "Assurance" means how well a Relying Party can be certain of the identity Binding between the Public Key and the entity whose Subject name is cited in the Certificate. In addition, it also reflects how well the Relying Party can be certain that the entity whose name is cited in the Subject of the Certificate is controlling the use of the Private Key that corresponds to the Public Key in the Certificate.

The level of Assurance associated with a Public Key Certificate describes the procedures and controls involved in validating a Subscriber's identity (see [VP](#)) and Binding that identity to a Public Key. It is the responsibility of the Relying Party to assess that level of Assurance and determine if it meets their security requirements for some particular use. The level of Assurance depends on the proper generation and management of the Certificate and associated Private Keys, in accordance with the stipulations of this CP. Personnel, physical, procedural, and technical security controls contribute to the Assurance level of the Certificates issued.

3.2.1 Method to Prove Possession of Private Key

The Authentication of the Subscriber, as defined in Section 3.2.3, is required prior to the proof of possession process described in this section.

In all cases where the Subscriber generates its own keys, that Subscriber SHALL prove possession of the Private Key, which corresponds to the Public Key in the Certificate Signing Request (CSR). For example, this MAY be done by the Subscriber, using its Private Key to sign the CSR or a value assigned by the RA. The RA SHALL then validate the signature using the Subscriber's Public Key provided in the CSR.

For cases where a trusted Account Administrator submits the CSR on behalf of the Subscriber, proof of possession MAY be done by the Subscriber using its Private Key to sign a value supplied by the CA. The CA SHALL describe in its CPS how it validates possession of the Private Key.

The PCA or ICA, and any RA on behalf of the CAs, SHALL prove that the Subscriber possesses the Private Key by verifying the Subscriber's Digital Signature on the PKCS #10 CSR with the Public Key in the CSR.

The PA MAY approve other methods to prove possession of a Private Key by a Subscriber that are at least as secure as those here.

3.2.2 Authentication of Organization Identity

The RA SHALL conform to the requirements contained within the [VP](#) to validate all identities, including organizations (agencies), devices and agents.

3.2.3 Authentication of Subscriber Identity

See [VP](#) Section 8.2.4: Verification of all Other Certificates and Section 8.9: Verified Method of Communication.

3.2.4 Non-verified Subscriber Information

Information that is not verified by a CA or RA SHALL NOT be included in Certificates.

3.2.5 Validation of Authority

The issuer CA SHALL validate the Subject CA Certificate requestor's authorization to act in the name of the Subject CA prior to issuing the CA Certificate in accordance to the verification requirements in the [VP](#). The Certificate issuance SHALL be based on a successful CA onboarding process (i.e., successful mapping of the CA Certificate information with this CP, successful CA CPS compliance analysis, approved architecture review, and PCA PA approval.)

3.2.6 Criteria for Interoperation

This CP provides for interoperability with third party CAs (i.e., CAs external to the PCA PKI) through cross-certification. The PA SHALL determine the criteria for cross-certification with other entities in accordance with the PCA PKI Cross-Certification Methodology and Criteria [forthcoming]. Interoperability will be established when directed by the PA and will require a Memorandum of Agreement (MOA) between the PCA and the third party CA.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

For Re-Key of any CA Certificate issued under this CP, the CA SHALL follow the same procedures as the initial registration process described in Section 3.2.

For Re-Key of any End-Entity Certificate issued under this CP, the RA SHALL follow the same procedures as the initial registration described in Section 3.2.

3.3.2 Identification and Authentication for Re-Key after Revocation

Once a Certificate has been Revoked for Compromise, the RA SHALL require a root cause analysis of the issue that led to Revocation, and a documented plan to address

the issue with committed dates. Issuance of a new Certificate and the Re-Key SHALL require completion of the plan and SHALL require following the same process as the initial registration process, described in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Revocation requests MUST be Authenticated by the PCA or ICAs, or their corresponding RAs, prior to the request being accepted. Requests to Revoke a Certificate MAY be Authenticated using that Certificate's Public Key, regardless of whether or not the associated Private Key has been Compromised. If the request cannot be Authenticated with the Certificate's Public Key, the CA or RA SHALL validate the information provided by the Revocation requestor and document those details prior to determining if the Revocation will be completed or not. The CA, or RA acting on its behalf, SHALL Authenticate a request for Revocation of a Certificate based on the information provided by the requestor. Authentication mechanisms used by the CA or RA SHALL balance the need to prevent unauthorized Revocation requests against the need to quickly Revoke Certificates. Revocation requests Authenticated on the basis of the current Key Pair SHALL always be accepted as valid, even if this Key Pair is the one suspected of being Compromised. Other Revocation request Authentication mechanisms MAY be used with the permission of the CA, such as challenge-response questions sent to the Certificate holder at the time of the Revocation request. All Revocation requests SHALL be logged by the CA or RA.

After a Certificate has been Revoked, other than during a Renewal or update action, the Subscriber SHALL go through the initial Certificate Application process to obtain a new Certificate.

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

The Certificate Application consists of the Subscriber agreement (i.e., the DCSA) and the accompanying Naming Application provided with the DCSA and an accompanying PKCS #10 CSR. A copy of the DCSA can be requested from the RA.

4.1.1 Who Can Submit a Certificate Application

No stipulation.

4.1.2 Enrollment Process and Responsibilities

Prospective Subscribers SHALL submit sufficient information to allow the PCA or ICAs, or their corresponding RAs, to successfully perform the required verification.

For the CA, or RA on its behalf, the identification and Authentication of the Subscriber MUST meet the requirements for Subscriber Authentication as specified in Section 3.2.

The CA or RA SHALL develop processes that sufficiently verify the Prospective Subscriber's identity for all Certificate types generated for the PCA PKI according to Section 3.2.

Prospective Subscribers SHALL:

- Agree to the applicable Subscriber agreement (i.e., the DCSA);
- Complete the Certificate Application provided in the DCSA;
- Provide the requested information;
- Respond to verification requests in a timely manner;
- Generate the Key Pair;
- Deliver the Public Key of the Key Pair to the RA; and
- Submit payment, if required.

The items in the list above MAY be completed in any order that is convenient for the RA and Prospective Subscribers that does not defeat security, but all SHALL be completed before Certificate issuance.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The RA SHALL perform the identification and Authentication validation functions for Prospective Subscribers requesting PCA PKI Certificates, as specified in Sections 3.2 and 3.3 in this CP.

4.2.2 Approval or Rejection of Certificate Applications

The RA SHALL approve a Certificate Application if all of the following conditions are met:

- Receipt of a fully executed DCSA;
- Receipt of a signed Certificate Application;

- Successful validation per the [VP](#);
- Receipt of all requested supporting documentation; and
- Payment (if applicable) has been received.

The RA SHALL reject any Certificate Application for which such validation cannot be completed, or when the RA has cause to lack confidence in the application. The RA MAY reject a Certificate Application if any one or more of the following conditions arise:

- The Prospective Subscriber fails to execute the required DCSA;
- An authorized representative fails to sign the Certificate Application;
- Unable to successfully validate per the [VP](#);
- The Prospective Subscriber fails to furnish requested supporting documentation;
- The Prospective Subscriber fails to respond to notices within a specified time;
- The Prospective Subscriber is not in good standing with the RA or CA;
- The RA believes that issuing the Certificate MAY bring the RA or CA into disrepute; or
- Payment (if applicable) has not been received.

The CA MAY reject any Certificate Application if the CA believes that issuing a Certificate MAY bring the CA into disrepute.

4.2.3 Time to Process Certificate Applications

RAs SHALL process Certificate Applications within ninety (90) days of receipt of all necessary documents as specified in the CPS.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

A Certificate is created and issued by a CA following its RA's approval of a Certificate Application. Upon receiving the request, the CA SHALL:

- Authenticate the RA using a Certificate provided to the RA by the CA;
- Receive the PKCS #10 CSR generated by the Subscriber from the RA;
- Generate a Certificate using the information in the CSR, along with any additional Certificate profile information provided by the RA; and
- Ensure delivery of the Certificate to the Subscriber.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificates

CAs issuing Certificates SHALL notify the RA of the creation of a Subscriber Certificate. The RA SHALL inform the Subscriber, through information submitted during the Certificate enrolment process, that their Certificate is available and the means for obtaining the Certificate.

4.4 Certificate Acceptance

Once downloaded, the Subscriber SHALL check the contents of the Certificate without delay. If the Subscriber detects any problems, the Subscriber SHALL notify the CA, or the RA on behalf of the CA, about the problem. The Certificates are considered

accepted thirty (30) days after the Certificate's issuance, unless the CA, or the RA on behalf of the CA, is notified of a problem.

4.4.1 Conduct Constituting Certificate Acceptance

An issued Certificate SHALL be deemed to have been accepted when it has been downloaded, installed, and used, and the Subscriber has not notified the RA of a problem with the Certificate or its contents.

4.4.2 Publication of the Certificate by the CA

CAs SHALL publish CA Certificates, as specified in Section 2.2.

This CP makes no stipulation regarding publication of Subscriber Certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

CAs operating under this CP SHALL notify PKI Participants whenever it issues a CA Certificate by updating its CA Repository.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber use of the Private Key corresponding to the Public Key in the Certificate SHALL only be permitted once the Subscriber has agreed to the DCSA and accepted the Certificate, as described in Section 4.4.1. Subscriber key use SHALL be consistent with the *keyUsage* and *extKeyUsage* extensions, in the associated Certificate.

Subscribers SHALL protect their Private Keys from unauthorized use and SHALL discontinue use of the Private Key following expiration or Revocation of the Certificate.

Subscriber Certificate use SHALL be in lawful accordance with the DCSA and the terms of this CP.

The RA SHALL provide guidance to Subscribers on its responsibilities on use of their Private Key and obtain the Subscriber's acknowledgement, as defined in Section 9.6.3.

4.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties SHALL independently assess the following:

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by Section 1.4;
- That the Certificate is being used in accordance with the *keyUsage* and *extKeyUsage* extensions included in the Certificate; and
- The status of the Certificate and all the CAs in the chain that issued the Certificate. If any of the Certificates in the Certificate chain have been Revoked, the Relying Party SHALL NOT rely on the Certificate or other Revoked Certificates in the Certificate chain.

4.6 Certificate Renewal

Renewing a Certificate means creating a new Certificate with the same name, key, and other information as the old one, but a new, extended Validity Period and a new serial number is created. Certificates are generally not Renewed in the PCA PKI, they are Re-Keyed (Section 4.7), however if a Certificate is Renewed the following sub-sections apply. Certificate Renewal does not violate the requirement for name uniqueness (see Section 3.1.5).

4.6.1 Circumstances for Certificate Renewal

Any Certificate MAY be Renewed if the Public Key has not reached the end of its Validity Period, the associated Private Key has not been Revoked or Compromised, and the Subscriber name and attributes are unchanged. In addition, the Validity Period of the Certificate MUST NOT exceed the remaining lifetime of the Private Key, as specified in Section 6.3.2.

Certificates MAY be Renewed as long as the aggregated lifetime of the Public Key does not exceed the Certificate lifetime specified in Section 6.3.2.

4.6.2 Who May Request Renewal

The following MAY request a Certificate Renewal:

- The Subscriber of the Certificate or an authorized representative of the Subscriber;
- A CA, to request a Renewal of its own Certificate; or
- A CA, to Renew its issued Certificates during recovery from a CA key Compromise.

4.6.3 Processing Certificate Renewal Requests

A CA MAY require a revalidation prior to Renewal of a Certificate.

When End-Entity Certificates are Renewed as a result of CA key Compromise, as described in Section 4.6.1, the CA or RA SHALL verify that all Certificates issued since the date of Compromise were issued appropriately. If the Certificate cannot be verified, then it MUST NOT be Renewed.

4.6.4 Notification of Certificate Renewal to Subscriber

The RA SHALL inform the Subscriber of the Renewal of its Certificate, in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Acceptance of the Renewed Certificate or its contents constitutes acceptance of the Certificate, as per Section 4.4.

4.6.6 Publication of the Renewal Certificate by the CA

Publication of Renewed Certificates is subject to the requirements in Section 2 of this CP.

4.6.7 Notification of Certificate Renewal by the CA to Other Entities

See Section 4.4.3.

4.7 Certificate Re-Key

Subscribers SHALL identify themselves to the RA for the purpose of Re-Keying as required in Section 3.

Certificate Re-Key consists of creating a new Certificate for a different Key Pair (and serial number) but can retain the contents of the original Certificate's *subjectDN*. Certificate Re-Key does not violate the requirement for name uniqueness (see Section 3.1.5). The new Certificate MAY be assigned a different Validity Period, key identifiers, and/or be signed with a different key.

4.7.1 Circumstances for Certificate Re-Key

When a CA Re-Keys a Certificate, the new Certificate MUST include a new key. A CA SHALL NOT process a Re-Key if the key is the same as the original. Any Certificate holder MAY request a Re-Key at any time.

A Certificate MAY be Re-Keyed after Revocation, for example, due to a Compromised Private Key. A Certificate MAY also be Re-Keyed before expiration to maintain continuity of Certificate usage. A Certificate MAY be Re-Keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key (Re-Key)

Requests to the RA for a new Public Key SHALL be considered for the following:

- Subscribers with a currently valid Certificate MAY request a new Public Key;
- The RA MAY request a new Public Key on behalf of a Subscriber;
- A CA MAY request a Re-Key of its own Certificate;
- A CA MUST Re-Key its issued Certificates during recovery from a CA key Compromise; or
- The appropriate PA MAY request Re-Key of CA Certificate.

4.7.3 Processing Certificate Re-Keying Requests

A CA MAY require a revalidation prior to Renewal of a Certificate.

4.7.4 Notification of New Certificate Issuance to Subscribers

A CA SHALL inform the Subscriber of the Re-Key of its Certificate, as per Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Acceptance of the Renewed Certificate or its contents constitutes acceptance of the Certificate, as per Section 4.4.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Publication of Re-Keyed Certificates is subject to the requirements in Section 2 of this CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

A CA SHALL treat all requests for Certificate Modification as new Certificate Applications, subject to the provisions of Sections 4.1 and 4.2.

Modifying a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old Certificate.

4.8.1 Circumstance for Certificate Modification

CA Certificates whose characteristics have changed (e.g., assert new policy OID) MAY be Modified. The new Certificate MAY have the same or a different Subject Public Key.

If the Modified Certificate will have the same Public Key as the original Certificate, the requirements for Renewal as stated in Section 4.6.1 also apply.

The RA MAY accept Certificate Modification requests only for Subscribers whose characteristics have changed in a way which would not invalidate the verification of identity used to issue the Certificate. The new Certificate MUST have a different Subject Public Key.

Certificates MAY be Modified:

- For a Subscriber organization name change or other Subscriber characteristic change; or
- For Validity Period.

A Certificate MAY be Modified after Certificate expiration.

4.8.2 Who May Request Certificate Modification

Requests to the RA for Certificate Modification SHALL be considered for the following:

- Subscribers with a currently valid Certificate MAY request Certificate Modification;
- The RA MAY request Certificate Modification on behalf of a Subscriber;
- A CA MAY request a Certificate Modification of its own Certificate; or
- The appropriate PA MAY request Modification of CA Certificates.

4.8.3 Processing Certificate Modification Requests

CA Certificate Modification SHALL be approved by the PA for the CA performing the Certificate Modification.

For Certificate Modification requests, the RA SHALL confirm the identity of the Subscriber in accordance with the requirements, as specified in the [VP](#).

4.8.4 Notification of Modified Certificate Issuance to Subscriber

A CA SHALL inform the Subscriber of the Modification of its Certificate, in accordance with Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Acceptance of the Modified Certificate or its contents constitutes acceptance of the Certificate, as per Section 4.4.

4.8.6 Publication of the Modified Certificate by the CA

Publication of Modified Certificates is subject to the requirements in Section 2 of this CP.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated Validity Period.

CAs SHALL issue CRLs covering all unexpired Certificates issued under this CP, except for OCSP responder Certificates that include the *id-pkix-ocsp-nocheck* extension.

CAs SHALL make public a description of how to obtain Revocation information for the Certificates they publish. The RA SHALL provide this information to Subscribers during the Certificate request or issuance and SHALL be readily available to any potential Relying Party.

The RA SHALL validate any Revocation requests subject to the requirements in Section Error! Reference source not found.. The RA MAY Authenticate requests to Revoke a Certificate using that Certificate's associated Public Key, regardless of whether the Private Key has been Compromised.

4.9.1 Circumstances for Revocation

The RA SHALL request from its corresponding CA that a Certificate be Revoked when the Binding between the Subject and the Subject's Public Key defined within the Certificate is no longer considered valid. When this occurs, the associated Certificate SHALL be Revoked. The CA SHALL include all Revoked Certificates on all new publications of the Certificate Status Service (CSS) information (see Section 4.10) until the Certificates expire.

Revocation SHALL occur on decision of the CA when reasonable and credible evidence exists to establish at least one of the following:

- A determination by the CA that Revocation is appropriate and/or needed;
- Identifying information or affiliation components of any names in the Certificate becomes invalid;
- Any information in the Certificate becomes invalid, subject to the terms of the CPS the Certificate is issued under;

- The Subscriber can be shown to have violated the stipulations of its DCSA or one or more sections of this CP;
- The original Certificate request was not authorized;
- The Subscriber or other authorized party asks for its Certificate to be Revoked;
- The Subscriber is no longer eligible to obtain a Certificate from a CA operating under this CP;
- The Certificate has been delivered based upon wrong or falsified information;
- There is reason to believe the Confidentiality of a Private Key is no longer ensured or has been Compromised; or
- The media holding the Private Key is suspected or known to have been Compromised.

If there is a Risk of a Private Key disclosure, then the CA SHALL Revoke the Certificate, and measures SHALL be taken to invalidate or securely erase the Private Key associated with the Certificate.

4.9.2 Who Can Request Revocation

Within the PKI, the Revocation of a Certificate MAY be requested by any one of the PKI Participants, including:

- The PCA PA MAY request the Revocation of any Certificate within the PCA PKI's domain. A written notice and brief explanation for the Revocation MUST subsequently be provided to the Subscriber;
- A CA MAY summarily Revoke Certificates it has issued. A written notice and brief explanation for the Revocation MUST subsequently be provided to the Subscriber;
- The RA MAY request the Revocation of a Subscriber's Certificate on the Subscriber's behalf;
- A Subscriber or sponsor of device Certificates MAY request Revocation of their own Certificates; and
- Relying Parties MAY request Revocation of any Certificate. The CA or RA SHALL investigate the request and present the results to the PCA PA for approval.

All Revocation requests MUST be Authenticated per Section Error! Reference source not found..

4.9.3 Procedure for Revocation Request

The Certificate Revocation requestor SHALL identify the date of the request, the Certificate to be Revoked, the reason for Revocation, and allow the requestor to be Authenticated.

Upon receipt of a Revocation request, the RA SHALL Authenticate the request and establish circumstances per Section 4.9.1.

The MA SHALL publicly disclose the instructions through a readily accessible online means, and in the CPS. The Issuer CA SHALL maintain a continuous twenty-four (24)

hours a day, seven (7) days a week ability to internally respond to any high priority Revocation requests.

Once Authenticated, the RA SHALL inform its corresponding CA and MA of the request. If the request for Revocation comes from someone other than the entities listed in Section 4.9.2, then the RA SHALL investigate the alleged basis for the Revocation request prior to informing the CA and MA of the request. In the event a Private Key is Compromised, time is of the essence to Revoke a Certificate. In that event, the CA MAY perform a Revocation without consulting the RA and MA.

The MA, at its discretion, MAY take whatever measures it deems appropriate to verify the need for Revocation. If the MA approves the Revocation, the MA SHALL direct the CA to Revoke the Certificate.

4.9.4 Revocation Request Grace Period

There is no grace period for Revocation under this CP.

Responsible parties SHALL request Revocation as soon as they identify the need for Revocation.

4.9.5 Time Within Which CA Must Process the Revocation Request

CAs SHALL process Certificate Revocation requests as quickly as practical upon receipt of a proper Revocation request from the RA. There is no stipulation about when Certificate Revocation requests are completed because such timing depends largely on the availability of information supporting authorization of the Revocation request.

The issuing CA SHALL Revoke a CA Certificate once all necessary approvals have been received and the proper notification periods have elapsed.

Issuing CAs SHALL Revoke Subscriber Certificates as quickly as practical upon receipt of a proper Revocation request.

Revocation requests SHALL be processed before the next CRL is published, excepting those requests validated within two (2) hours of CRL issuance. Revocation requests validated within two (2) hours of CRL issuance MUST be processed before the following CRL is published.

The Issuer CA SHALL maintain a continuous twenty-four (24) hours a day, seven (7) days a week ability to internally respond to any high priority Revocation requests.

4.9.6 Revocation Checking Requirement for Relying Parties

A Relying Party MUST obtain the current CRL or employ the CSS provided by its CA to determine if a Certificate has been Revoked.

CAs, MAs, and RAs SHALL provide Relying Parties with information on how to find the appropriate CRL or web-based Repository, or CSS to check the Revocation status of Certificates issued by the CA.

Relying Parties SHOULD maintain a local OCSP server in the event Certificate status checking is not available (which can be caused by any number of different reasons such

as lack of local network connectivity or Internet outage, no CRL/OCSP server availability, missing CRL file at the CSS, etc.). A cache of the CRL MAY be maintained locally.

Fallback operation, in the event Certificate status checking is not available, SHOULD use the cached version of the CRL until the latest CRL can be downloaded or the online availability of CSS is restored. If a cached version of the CRL is not available, the Certificate SHOULD be considered valid until its status can be checked in the next available CRL or via the online CSS.

4.9.7 CRL Issuance Frequency

A CA SHALL generate and publish (a.k.a. issue) CRLs periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information MAY be issued more frequently than the issuance frequency described below. A CA SHALL ensure that superseded Certificate status information is removed from the PKI Repository upon posting of the latest Certificate status information. Furthermore, all pre-generated CRLs not yet published SHALL be securely destroyed whenever the CA Revokes any Certificate.

Certificate status information SHALL be published no later than the next scheduled update. This will facilitate the local caching of Certificate status information for offline or remote operation. The CA SHALL update its PKI Repositories to which they post Certificate status information to reduce latency between creation and availability.

Table 3 below provides CRL issuance frequency requirements.

Table 3: CRL Issuance Frequency

Type of CRL	Issuance Frequency
Routine	At least once every twenty-four (24) hours
Loss/Compromise of Private Key (Emergency)	Within four (4) hours of notification
CA Compromise (Emergency)	Immediately, but no later than within fifteen (15) minutes of generation.

CRL issuance frequency requirements MAY be further constrained by applicable jurisdictional regulatory law.

The CAs that issue routine CRLs less frequently than the requirement for emergency CRL issuance (i.e., CRL issuance for loss or Compromise of key or for Compromise of CA) SHALL meet the requirements specified above for issuing emergency CRLs.

4.9.8 Maximum Latency for CRLs

A CA SHALL publish CRLs within four (4) hours of generation, except for CA Compromise emergencies, which SHALL be published immediately, but no later than within fifteen (15) minutes of generation. Furthermore, each CRL SHALL be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for the same scope.

The maximum delay between the time a Certificate Revocation is performed by a CA and the time that this Revocation information is available to Relying Parties SHALL be no greater than fifteen (15) minutes.

4.9.9 Online Revocation/Status Checking Availability

CAs SHALL have a web-based Repository that permits Relying Parties to make online inquiries regarding Revocation and other Certificate status information. CAs SHALL provide Relying Parties with information on how to find the appropriate Repository to check Certificate status and how to find the correct OCSP responder.

All online CRLs SHALL have service availability of not less than 99.95% with scheduled downtime notification of at least thirty (30) hours in advance. Scheduled downtime for online CRLs SHALL NOT exceed four (4) hours in any single calendar week, or sixteen (16) hours in a calendar year.

4.9.10 Online Revocation Checking Requirements

Relying Party client software SHOULD support online status checking. Client software using online status checking is NOT required to obtain or process CRLs.

A Relying Party SHOULD check the status of a Certificate on which they wish to rely. If a Relying Party does not check the status of a Certificate by consulting the most recent CRL, the Relying Party SHOULD check the Certificate status by consulting the applicable online Repository or by requesting Certificate status using the applicable OCSP responder.

4.9.11 Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate Revocation information SHALL be described in the CA's CPS and SHALL be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and online Revocation and status checking. CRL and OCSP Certificate status checking SHALL be supported even if alternate mechanisms are provided.

4.9.12 Special Requirements Regarding Key Compromise

See Section 4.9.3.

A CA SHALL notify its PA in the event of Compromise, or suspected Compromise, of the CA Private Key.

4.9.13 Circumstances for Suspension

Suspension is not supported by this CP.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services (CSS)

The PCA PKI MUST include a service that provides status information about Certificates on behalf of a CA through online transactions. In particular, the PCA PKI includes CRLs and OCSP responders to provide online status information. Such a service is termed a Certificate Status Service (CSS). Where the CSS is identified in Certificates as an authoritative source for Revocation information or issued a delegated responder Certificate, the operations of that authority are considered within the scope of this CP. A CSS SHALL assert all the policy OIDs for which it is authoritative, including OCSP servers that are identified in the Authority Information Access (AIA) extension. OCSP servers that are locally trusted, as described in [RFC 2560](#), are not required to meet Section 4.10.2 below.

The CSS is considered an integral part of the CAs and, except where expressly noted, all requirements imposed on CAs apply.

4.10.1 Operational Characteristics

A CSS SHALL meet the following requirements:

- The CSS SHALL be operated in compliance with this CP;
- Information exchanged between a CA and the CSS SHALL be Authenticated and protected from Modification using mechanisms commensurate with the requirements of the data to be protected by the Certificate being issued;
- Accurate and up-to-date information from the associated CA SHALL be used to provide the Revocation status;
- Revocation status responses SHALL provide Authentication and Integrity services commensurate with the requirements of the data to be protected by the Certificates being issued, to include the status of the Certificate and the time the status indication was generated; and
- Latency of Certificate status information SHALL meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

Certificate status can be ascertained by querying the CRL maintained and published in its Repository by the CA, or by querying an authorized OCSP responder.

4.10.2 Service Availability

Relying parties SHOULD establish instances of a trusted OCSP responder. A CA's OCSP service SHALL be available twenty-four (24) hours a day, seven (7) days a week, fifty-two (52) weeks a year, with the following availability:

- Outside declared maintenance window: 99.99%
- Within declared maintenance window: 99.9%

Declared maintenance windows SHALL NOT exceed four (4) hours in any single calendar week.

Relying Parties MAY locally cache CRLs for cases where the Relying Party is not able to Access the Certificate status online.

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

Subscription is synonymous with the Certificate Validity Period. The subscription ends when the Certificate is Revoked or expired.

For Certificates that have expired prior to or upon end of subscription, Revocation is not required. Issuing CAs SHALL always Revoke unexpired CA Certificates at the end of the subscription.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

All entities performing CA functions SHALL implement and enforce the following physical, procedural, logical, and personnel security controls for a CA.

5.1 Physical Controls

The CA SHALL protect all CA equipment, including Cryptographic Modules from theft, loss, and unauthorized Access. Unauthorized use of CA equipment is prohibited. The CA SHALL dedicate CA equipment to performing CA functions. The CA SHALL implement physical Access Controls to reduce the Risk of equipment tampering, even when the Cryptographic Module is not installed and activated.

All the physical control requirements specified below apply equally to the PCA and ICAs.

5.1.1 Site Location and Construction

The CA SHALL conduct all CA operations within a physically protected environment that deters, prevents, and detects unauthorized use of, Access to, or disclosure of sensitive information and systems. The CA SHALL select its site location and construction, so that when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, it SHALL provide robust protection against unauthorized Access to the CA equipment and Records.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

The CA SHALL have physical Access Controls for CA equipment, as well as remote workstations used to administer the CAs, to:

- Protect all CA equipment from unauthorized Access;
- Manually or electronically monitor CA equipment for unauthorized intrusion;
- Ensure an Access log is maintained and available for inspection by internal as well as external Auditor;
- Store all removable media and paper containing sensitive plain-text information in secure containers; and
- Require two (2)-person physical Access Control to both the Cryptographic Module and computer systems.

The CA SHALL place all removable Cryptographic Modules and the activation information used to Access or enable Cryptographic Modules in secure containers when not in use. Activation Data SHALL be either memorized or recorded and stored in a manner commensurate with the security afforded the Cryptographic Module, and SHALL NOT be stored with the Cryptographic Module or removable hardware associated with remote workstations used to administer the CA. Access to the contents of the locked containers SHALL be restricted to individuals holding CA Trusted Roles, as defined in Section 5.2.1, utilizing two (2)-person Access Controls, and two (2)-person Integrity while the container is unlocked.

When in active use, the Cryptographic Module SHALL be locked into the system or container (rack, reader, server, etc.) using a physical lock under the control of the CA Operations Staff to prevent unauthorized removal.

A security check of the CA Facility, or remote workstations used to administer the CAs, SHALL occur prior to leaving the CA Facility unattended. The check SHALL verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that Cryptographic Modules are in place when "open," and secured when "closed," and for the CA, that all equipment other than the Repository/CSS is shut down);
- Any containers housing the Cryptographic Module are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized Access.

If the facility is not continuously attended, the last person to depart must initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

The RA SHALL protect its RA equipment from unauthorized Access.

5.1.3 Power and Air Conditioning

The CA SHALL have facilities equipped with primary and Backup power systems to ensure continuous, uninterrupted Access to electric power sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

The CA SHALL install its equipment such that it prevents damage from exposure to water. The CA SHALL construct its facilities and SHALL implement procedures to prevent floods or other damaging exposure to water. Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

The CA SHALL equip its facilities with fire suppression mechanisms. These measures SHALL meet all local applicable safety regulations.

5.1.6 Media Storage

The CA SHALL store its media to protect it from accidental damage (water, fire, electromagnetic) and prevent unauthorized physical Access. The CA SHALL store media not required for daily operation, or not required by policy, to remain with the CA that

contains security Audit, Archive, or Backup information in a securely stored location separate from the CA equipment.

5.1.7 Waste Disposal

The CA and RA SHALL destroy sensitive media and documentation that are no longer needed for operations in a secure manner, for example, sensitive documentation SHALL be shredded, burned, or otherwise rendered unrecoverable.

Destruction of media and documentation containing sensitive information, such as Private Key material, MAY employ methods commensurate with those in the NIST Guidelines for Media Sanitization [[SP 800-88-1](#)].

5.1.8 Off-Site Backup

The CA SHALL maintain full system Backups and make regular Backup copies of any information necessary to recover from system failure, on a periodic schedule. The CA SHALL store at least one full Backup copy at an off-site location (separate from CA equipment). The CA SHALL store the Backup at a site with physical and procedural controls commensurate to that of the operational CA system.

5.2 Procedural Controls

Procedural controls are requirements on Trusted Roles that perform functions that can introduce security problems, either accidentally or maliciously, if not carried out properly. The functions performed in these roles form the basis of trust for the entire PKI.

5.2.1 Trusted Roles

Trusted Persons are personnel identified to fill Trusted Roles and are designated to manage the PKI's trustworthiness.

Two (2) approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. Trusted Persons include all employees, contractors, and consultants that have Access to or control Authentication or cryptographic operations that MAY materially affect:

- The validation, Authentication, and handling of information in Certificate Applications;
- The acceptance, rejection, or other processing of Certificate Applications, Revocation requests, Renewal requests, or enrollment information;
- The issuance, or Revocation of Certificates, including (in the case of workstations) personnel having Access to restricted portions of its Repository;
- Access to safe combinations and/or keys to security containers that contain materials supporting production services;

- Access to Hardware Security Modules (HSMs), their associated keying material, and the secret share splits of the Personal Identification Numbers (PINs) that protect Access to the HSMs;
- Installation, configuration, and maintenance of the CA;
- Access to restricted portions of the Certificate Repository;
- The handling of Subscriber information or requests; and
- The ability to grant physical and/or logical Access to the CA equipment.

A Trusted Role is one who performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Thus, it is essential that the people selected to fill these roles SHALL be held accountable to perform designated actions correctly or the Integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA.

Multiple people MAY hold the same Trusted Role, with collective privileges sufficient to fill the role. CAs MAY use different titles to describe these roles, or break out the duties in different ways, as long as the requirements for separation of duties are met (see Sections 5.2.2 and 5.2.4). Other Trusted Roles MAY be defined by the organization administering the PKI, in which case they will be described as additional subsections below.

5.2.1.1 CA Administrator

The CA Administrator SHALL maintain lists, including names, organizations, contact information, and organizational affiliation for those who perform CA Administrator functions.

The CA SHALL ensure a separation of duties into Trusted Roles for critical CA functions to prevent an individual from maliciously using the CA system without detection. Each such Trusted Role's system Access is to be limited to those actions which they are REQUIRED to perform in fulfilling their responsibilities.

The CA Administrator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring CA Audit parameters;
- Configuring Certificate status information;
- Generating and backing up CA keys;
- Controlling and managing CA Cryptographic Modules;
- System Backups and recovery;
- Changing recording media; and
- Posting Certificates and CRLs.

The individual with Access to the Private Keys SHALL NOT have security Audit responsibilities, nor be able to generate system Backups and recovery. The person who generates system Backups and recovery SHALL NOT have Access to the Private Keys, and SHALL NOT have security Audit responsibilities.

5.2.1.2 CA Operations Staff

The CA Operations Staff role is responsible for issuing Certificates. The CA SHALL maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in CA Administrator, CA Operations Staff, and Security Auditor Trusted Roles.

The CA Operations Staff role includes:

- Managing operations of hosted CAs;
- Authenticating RAs;
- Executing the issuance of Certificates requested by the RA;
- Approving and executing Certificate Revocation requests;
- Approving Certificates issued to support the operations of the CA;
- Providing Certificate Revocation status information;
- Generating Certificate issuance reports; and
- Configuring Certificate profiles or templates.

5.2.1.3 Security Auditor

Security Auditors (i.e., internal Auditors) are responsible for internal Auditing of CAs and RAs. This sensitive role SHALL NOT be combined with any other sensitive role, e.g., the Security Auditor SHALL NOT also be part of the CA Operations Staff or CA Administrator. Security Auditors SHALL review, maintain, and Archive Audit logs, and perform or oversee internal Audits (independent of formal Compliance Audits) to ensure that CAs are operating in accordance with this CP.

5.2.1.4 RA Staff

RA Staff are the individuals holding Trusted Roles that operate and manage RA components. The RA SHALL maintain lists, including names, organizations, and contact information of those who act in RA Staff, RA Administrator, and RA Security Auditor Trusted Roles for that RA.

RA Staff is responsible for the following:

- Installation, configuration, and maintenance of RA equipment;
- Establishing and maintaining RA operating system and application accounts;
- Routine operation of the RA equipment such as system Backup and recovery or changing recording media;
- Registering new Subscribers and requesting the issuance of Certificates;
- Verifying the identity of Subscribers;
- Verifying the accuracy of information included in Certificates;
- Approving and executing the issuance of End-Entity Certificates;
- Requesting, approving, and executing Revocation of Certificates;
- Securely communicating requests to, and responses from, the CA; and
- Receiving and distributing Subscriber Certificates.

The RA SHALL ensure a separation of duties into Trusted Roles for critical RA functions to prevent an individual from maliciously using the RA system without detection. Each

such Trusted Role's system Access is to be limited to those actions which they are REQUIRED to perform in fulfilling their responsibilities.

5.2.2 Number of Persons Required per Task

Multi-person control procedures are designed to ensure that, at a minimum, two (2) Trusted Persons are present to gain either physical or logical Access to the CA. The CA SHALL enforce multi-person Access to CA Cryptographic Modules, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA is activated with operational keys, further Access Controls SHALL be invoked to maintain split control over both physical and logical Access to the CA. Persons with physical Access to CA modules SHALL NOT hold credentials to activate the CA and vice versa.

Two (2) or more persons are required for the following tasks:

- Access to CA hardware;
- Management of CA cryptographic hardware;
- CA key generation;
- CA Private Key activation; and
- CA Private Key Backup.

Where multi-person control is required, at least one (1) of the PKI Participants SHALL be an administrator. The PKI Participants defined in Section 5.2.1 SHALL serve in a Trusted Role. Multi-person control SHALL NOT be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3 Identification and Authentication for Each Role

Individuals assigned to Trusted Roles SHALL be appointed to the Trusted Role by an appropriate approving authority. Identity proofing of CA Trusted Roles SHALL be performed by the CA. The identity proofing of RA Trusted Roles SHALL be performed by the RA. Verification of identity SHALL include the personal (physical) presence of such personnel before human resources or other personnel performing security functions through either a face-to-face meeting or through a trusted video conferencing process approved by the PA and a check of well-recognized forms of identification, such as passports and driver's licenses. These appointments SHALL be annually reviewed for continued need and renewed if appropriate. The CA and RA SHALL record the Trusted Role approvals in a secure and Auditable fashion. Individuals holding Trusted Roles SHALL accept the responsibilities of the Trusted Role, and the CA/RA SHALL record this acceptance in a secure and Auditable fashion.

CAs SHALL confirm the identity and authorization of all personnel seeking to become Trusted Persons before such personnel are:

- Issued Access devices and granted Access to the required CA Facilities; and
- Given electronic credentials to Access and perform specific functions on CA systems.

CA equipment SHALL require, at a minimum, strong Authenticated Access Control for remote Access using multi-factor Authentication. Examples of multi-factor

Authentication include: use of a password or PIN along with a time-based token, digital Certificate, or other device that enforces a policy of what a user has and what a user knows.

5.2.4 Roles Requiring Separation of Duties

An individual that performs any Trusted Role SHALL only have one identity when Accessing CA or RA equipment. The PCA, ICAs, and the corresponding RAs on their behalf SHALL have procedures to ensure that no user identity can assume multiple roles.

Roles requiring separation of duties include, but are not limited to:

- Processing and approval of Certificate Applications, and Revocation requests;
- Issuance or Revocation of Certificates, including personnel having Access to restricted portions of the Repository;
- Generation of Backups;
- Generation, issuance, or destruction of a CA Certificate Private Key;
- Loading of a CA to a production environment; and
- Security Auditor role.

Role separation, when required as mentioned above, MAY be enforced by either the CA or RA equipment, or procedurally, or by both means.

5.3 Personnel Controls

Personnel controls plays a critical role in the PKI's overall system security to prevent unauthorized Access to CA and RA systems and CA/RA operations.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking Trusted Roles SHALL present proof of the requisite qualifications and experience to perform their duties, or be provided the training needed, to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any Trusted Role SHALL:

- Have no other duties that would interfere or conflict with their responsibilities, as defined in Section 5.2.1;
- Have demonstrated the ability to perform their duties;
- If necessary, have successfully completed the appropriate training; and
- Have not been previously relieved of Trusted Role duties for reasons of negligence or non-performance of duties.

5.3.2 Background Check Procedures

The CA and RA SHALL select persons filling Trusted Roles on the basis of loyalty, trustworthiness, and Integrity, and SHALL subject the persons to a background investigation.

The CA and RA SHALL conduct background checks (in accordance with local Privacy laws) for the previous five (5) years, which MAY include a combination of the following:

- The person is an employee of, or contractor of, the CA or RA and is bound by terms of employment or contract;
- Confirmation of employment history;
- Check of previous places of residences over the past three (3) years;
- Check of professional reference;
- Confirmation of the highest or most relevant educational degree obtained;
- Search of criminal Records (local, state or provincial, and national);
- Search of driver's license Records;
- Identification verification (e.g., driver's license, passport); and
- Any other applicable procedures followed by a public safety agency for critical employees in the jurisdiction the CA/RA covers.

CAs and RAs SHALL have a process in place to ensure employees in Trusted Roles undergo background checks at least every ten (10) years.

5.3.3 Training Requirements

The CA and RA SHALL provide their personnel with the training needed to perform their job responsibilities competently and satisfactorily. The CA and RA SHALL conduct training in the following areas:

- Basic PKI knowledge;
- Security principles and mechanisms;
- PKI hardware and software versions in use on the CA systems;
- PKI duties the Trusted Role is expected to perform; and
- Disaster recovery and business continuity procedures.

The CA and RA SHALL document the identity of all personnel who received training and the level of training completed.

5.3.4 Retraining Frequency and Requirements

The CA and RA SHALL provide refresher training and updates, at least annually, for all individuals in Trusted Roles to ensure that such personnel maintain the required level of proficiency to perform their role. The CA and RA SHALL:

- Make individuals in Trusted Roles aware of changes in the operations of the PKI, this CP, or the CPS;
- Plan and document training for any significant change to the PKI operations, this CP, or the CPS and;
- Document the identity of all personnel who receive training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

Job rotation MUST NOT violate role separation. All Access rights associated with a previous role MUST be terminated.

All job rotations MUST be documented. Individuals assuming a Compliance Auditor role MUST NOT Audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

The CA and RA SHALL establish, maintain, and enforce policies for the discipline of personnel following unauthorized actions. The CA and RA disciplinary actions MAY include measures up to and including termination and SHALL be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

The CA and RA MAY permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly defined outsourcing needs. Contractors fulfilling Trusted Roles SHALL follow all personnel requirements stipulated in this CP and SHALL establish procedures to ensure that their duties are in accordance with this CP.

The CA SHALL escort independent contractors and consultants not fulfilling a Trusted Role and directly supervise them with Trusted Persons when they are given Access to the CA Facility, or CA and RA systems.

5.3.8 Documentation Supplied to Personnel

The CA and RA SHALL make available to its personnel this CP, the corresponding CPS, and any relevant statutes, policies, or contracts needed for the Trusted Persons to perform their duties.

5.4 Audit Logging Procedures

The CA and RA SHALL generate Audit log files for all events relating to the security of the CA and RA.

Where possible, the Audit logs MUST be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism MUST be used. All Audit logs, both electronic and non-electronic, MUST be retained and made available during Compliance Audits. Implementation and documentation of automated tools MUST describe how relevant events and anomalies are recorded.

Audit Record reviews SHOULD be performed using an automated process, and MUST include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities.

A Record of the review, all significant events, and any actions taken as a result of these reviews MUST be explained in an Audit log summary. This review summary MUST be retained as part of the long-term Archive.

5.4.1 Types of Events Recorded

The CA and RA SHALL include in each Audit Record the following information (either recorded automatically or manually for each Auditable event):

- The type of event;
- The date and time the event occurred;
- Success or failure; and

- The identity of the entity and/or person that caused the event.

The CA and RA SHALL enable all security Auditing capabilities of the CA and RA operating systems and applications to record the following events (where these events cannot be electronically logged, the CA and RA SHALL supplement the electronic Audit logs with physical logs as necessary):

Table 4: Auditable Events Recorded

Auditable Event	CA	RA
<i>Physical Access to CA Facility:</i>		
Personnel Access to room housing CA	X	
Access to the CA server	X	
Known or suspected violations of physical security	X	
Any removal or addition of equipment to the CA enclosure	X	
Power outages including UPS failure	X	
<i>System Configuration:</i>		
Installation of the operating system	X	
Software check Integrity failures	X	
Installation of the CA software	X	
Installation and removal of hardware Cryptographic Modules	X	
System startup	X	
Any security-relevant changes to the configuration of the CA	X	
Any changes to the Audit parameter, e.g., Audit frequency	X	
CA hardware configuration	X	
System configuration changes and maintenance	X	
Cryptographic Module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement)	X	
<i>Account Administration:</i>		
Roles and users are added or deleted	X	
The Access Control privileges of a user account or a role are modified	X	
Appointment of an individual to a Trusted Role	X	
Designation of personnel for multi-person control	X	
System administrator accounts	X	
Attempts to create, remove, set passwords, type of authenticator (e.g., from token to password), or change the system privileges of the privileged users (Trusted Roles)	X	
Attempts to delete or modify Audit logs	X	
Changes to the value of maximum Authentication attempts	X	
Resetting operating system clock	X	
Any changes to the Audit parameter, e.g., Audit frequency	X	
<i>CA Operational Events:</i>		
Key generation	X	

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Auditable Event	CA	RA
The export of CA Private Keys	X	
Start-up and shutdown of CA systems and applications	X	
Changes to CA details or keys	X	
Records of the destruction of media containing key material, Activation Data, or personal Subscriber information	X	
Successful and unsuccessful attempts to log into the CA system	X	
The value of maximum Authentication attempts is changed	X	
Maximum unsuccessful Authentication attempts occur during user login	X	
A CA Administrator unlocks an account that has been locked as a result of unsuccessful Authentication attempts	X	
Attempts to set passwords	X	
Attempts to modify passwords	X	
Access, backing up, or restoring the CA internal database	X	
Violations of CP or CPS stipulations	X	X
<i>End-Entity Certificate Lifecycle Events:</i>		
Certificate Application requests		X
Certificate requests	X	X
Issuance	X	
Re-Key	X	X
Renewal	X	X
Certificate Revocation requests	X	X
Revocation	X	X
Changes to Certificate profiles	X	
<i>Trusted Person Events:</i>		
Logon and logoff to the CA system	X	X
Attempts to create, remove, set passwords or change the system privileges of the privileged users	X	X
Unauthorized attempts to Access the CA system	X	X
Unauthorized attempts to Access system files	X	X
Failed read and write operations on the Certificate	X	
Personnel changes	X	X
Account Administrator Certificates	X	X
<i>Data Events:</i>		
Any attempt to delete or modify critical files (e.g., Audit log)	X	X
All successful and unsuccessful requests for confidential and security-relevant Information	X	X
Posting material to Repository	X	

5.4.2 Requirements for Time-Stamping of Audit Records

The CA and RA SHALL automatically time-stamp Audit Records as they are created. The CA and RA SHALL describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.4.3 Frequency of Processing Log

The CA SHALL review the Audit log at least once every thirty (30) days, unless the CA is offline, in which case the Audit logs SHALL be reviewed when the system is activated or every sixty (60) days, whichever is later.

The RA SHALL review its Audit logs at least once per quarter.

The CA and RA external Audit reviews SHALL involve verifying that the logs have not been tampered with, that there is no discontinuity or other loss of Audit Data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

5.4.4 Retention Period for Audit Log

Audit Records MUST be accessible until reviewed, in addition to specific Records being Archived as described in Section 5.5. The Security Auditor SHALL be only the entity who removes Audit logs from the CA system.

The CA and RA SHALL make all Audit logs, both electronic and non-electronic, available during a Compliance Audit.

5.4.5 Protection of Audit Logs

The CA and RA SHALL protect Audit logs from unauthorized viewing, modification, deletion, or other tampering. CA and RA system configuration and procedures SHALL be implemented together to ensure that only authorized people Archive or delete Audit logs. The CA and RA SHALL implement procedures to protect Archived data from deletion or destruction.

System configuration and operational procedures SHALL be implemented together to ensure that:

- Only authorized personnel have read Access to the logs;
- Only authorized personnel MAY Archive Audit logs;
- Audit logs are not modified; and
- Audit logs are stored in a secure storage.

5.4.6 Audit Log Backup Procedures

The CA and RA SHALL Backup their Audit logs and Audit summaries at least monthly, unless the CA is offline, in which case Audit logs and Audit summaries SHALL be backed up every time the system is activated, or at least every thirty (30) days.

5.4.7 Audit Collection System (Internal vs. External)

The Audit log collection system MAY or MAY NOT be external to the CA or RA system.

Where possible, the CA and RA SHALL automatically collect Audit logs. Where this is not possible, the CA and RA SHALL use a logbook, paper form, or other physical mechanism. Automated Audit processes SHALL be invoked at system or application start-up, and cease only at system or application shutdown. Audit collection systems SHALL be configured such that the Audit log is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated Audit system has failed; CA and RA operations SHALL be suspended until the Audit capability can be restored.

5.4.8 Notification to Event-Causing Subject

This CP has no stipulation to notify the individual, organization, or device that caused an event that an event was Audited.

5.4.9 Procedures to Obtain and Verify Audit Log Information

After receiving a request made for a proper entity, its agent, or a party involved in a dispute over a transaction involving the PKI, the CA, or RA MAY elect to retrieve the information from its Audit Log system. The CA or RA SHALL verify the Integrity of the Audit Log information. The CA or RA MAY elect to transmit the relevant information via a secure electronic method or courier.

5.4.10 Vulnerability Assessments

The CA and RA SHALL perform routine self-assessments of security controls for vulnerabilities that identify and assess reasonably foreseeable internal and external Threats that could result in unauthorized Access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate issuance process. The CA and RA SHALL perform their assessments, at least on an annual basis (e.g., as part of a WebTrust Audit), as input into their annual Audit.

5.5 Records Archival (Retention)

5.5.1 Types of Records Archived

Archived (or retained) Records SHALL be sufficiently detailed to determine that functions of the MA, CA, and RA have been properly executed. At a minimum, the following data SHALL be recorded and retained:

Table 5: Records Retention

Records to be Retained	CA	RA	MA
CP			X
CA Certificates issued and Key Pairs	X		
Export of CA Private Keys	X		
CPS	X		X
Agreements (e.g., Subscriber Agreements)	X	X	X
Modifications and updates to CA system or configuration	X		
Subscriber identity verification data as per Section 3.2.3		X	

Records to be Retained	CA	RA	MA
CRLs issuance	X		
Certificates issued, Re-Keyed, Renewed, and Revoked	X		
Audit logs	X	X	
Compliance Auditor reports (e.g., Audit summary report)	X		
Any attempt to delete or modify the Audit logs	X		
Remedial action taken as a result of violations of physical security	X		
Certificate request documentation		X	
Appointment of an individual to a Trusted Role	X	X	
Destruction of Cryptographic Modules	X		
Certificate Compromise notifications	X	X	
Any changes to the Audit parameters, e.g., Audit frequency, type of event Audited	X	X	X
The approval or rejection of a Certificate status change request	X	X	
Violations of Certificate Policy			X
Violations of Certification Practice Statement			X

5.5.2 Retention Period for Archive

Archive retention periods begin at the key generation event for any CA. For CAs that leverage key-rollover procedures a new retention period begins for each subsequent key generation event.

CAs SHALL maintain all Archived Records related to that CA, in an accessible fashion, for three (3) years after CA expiration or CA termination.

Individual RA Records associated with Certificate request Authorization, Certificate Revocation, Subscriber Authentication, or Subscriber Certificate acceptance MUST be maintained for a minimum of three (3) years after the Subject Certificate expiration date. Issuance of new Certificates with extended Validity Periods (i.e., Renewal, Re-Key or Modification) supported by existing Subscriber Authentication Records (i.e., Authentication using an existing valid Certificate) will result in a new retention period for those initial Records, based on the new Certificate expiration date.

5.5.3 Protection of Archive

The CA, RA, and MA SHALL protect the Records so that only authorized Trusted Persons are able to obtain Access to the Records. The Records SHALL be protected against unauthorized viewing, modification, deletion, or other tampering. The Recorded media and the applications required to process the Records SHALL be maintained to ensure that the Records can be Accessed for the retention time period.

5.5.4 Archive Backup Procedures

CAs and RAs compiling Records information SHALL incrementally back up the Records information at least on a weekly basis and perform full Backups at least on a monthly basis. Copies of paper-based Records SHALL be maintained in secure storage.

5.5.5 Requirements for Time-Stamping of Records

The CA and RA SHALL automatically time-stamp Records as they are created. The CA and RA SHALL describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

The CA SHALL collect Records information internally.

5.5.7 Procedures to Obtain and Verify Archive Information

After receiving a request made for a proper entity, its agent, or a party involved in a dispute over a transaction involving the PKI, the CA or RA MAY elect to retrieve the information from its Records system. The CA or RA SHALL verify the Integrity of the Records information. The CA or RA MAY elect to transmit the relevant information via a secure electronic method or courier.

5.6 Key Changeover

To minimize Risk from Compromise of a CA's Private Key, that key MAY be changed in accordance with the CPS. From that time on, only the new key will be used to sign Certificates. If the old Private Key is used to sign OCSP responder Certificates or CRLs that cover Certificates signed with that key, the old key MUST be retained and protected.

The CA's Private Key SHALL have a Validity Period as described in Section 6.3.2 and MAY be Re-Keyed at any time during its Validity Period, as per Section 4.7.

If an Intermediate CA is to be Re-Keyed, the Intermediate CA SHALL generate a new Public Key Pair and submit a CSR to the PCA to request its Intermediate CA Certificate. The Intermediate CA SHALL notify entities relying on its Certificate that its CA Certificate has been Re-Keyed. The PCA SHALL publish the issued CA Certificate in its Repository. The new Intermediate CA Private Key is used to re-sign all active End-Entity Certificates it has issued.

When the PCA Certificate is to be Re-Keyed, the PCA SHALL generate a new Key Pair and two (2) Key Rollover Certificates:

- One (1) Key Rollover Certificate where the new Public Key is signed by the old Private Key, indicating that this is the new PCA Public Key; and
- The other Key Rollover Certificate where the old Public Key is signed with the new Private Key, indicating that this is the old Public Key being replaced.

The new PCA Certificate will be available for download from the new PCA's Repository. The Relying Party will validate both Certificates and replace the old PCA Certificate with

the published new PCA Certificate. This permits acceptance of newly issued Certificates and CRLs without distribution of the new self-signed Certificate to current users.

The new PCA Private Key is used to re-sign all existing active Intermediate CAs, which then issue new End-Entity Certificates. There is no need to re-sign existing active End-Entity Certificates, unless the Intermediate CA is also Re-Keyed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA and RA SHALL have an Incident Response Plan and a Disaster Recovery Plan (DRP).

If Compromise of a CA is suspected, the CA SHALL stop Certificate issuance and follow the procedures outlined in Section 5.7.3. The CA SHALL assess the scope of potential damage in order to determine appropriate remediation procedures.

In case of a CSS key Compromise, all Certificates issued to the CSS SHALL be Revoked and the Revocation information SHALL be published immediately in the most expeditious manner. Subsequently, the CSS SHALL be Re-Keyed.

The CA SHALL notify the MA, PA and (if applicable) ICA PA if any CAs operating under this CP experiences the following:

- Suspected or detected Compromise (including Compromise of the CA's Private Key) of the CA systems;
- Physical or electronic penetration of CA systems;
- Successful denial of service attacks on CA components; or
- Any incident preventing the CA from issuing a CRL within twenty-four (24) hours of the issuance of the previous CRL.

The CA SHALL re-establish operational capabilities as quickly as possible.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this CP SHALL respond as follows:

- Notify the MA, PA and (if applicable) ICA PA and other CAs as soon as possible;
- Ensure that the system's Integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of Backup;
- Re-establish CA operations, giving priority to the ability to generate Certificate status information within the CSS and CRL issuance schedule;
- If the CA Private Keys are not destroyed, CA operation SHALL be re-established, giving priority to the ability to generate Certificate status information within the CSS and CRL issuance schedule;
- If the CA Private Keys are destroyed, re-establish CA operations as quickly as possible, giving priority to the generation of a new CA Key Pair;

- If the Integrity of the system cannot be restored, or if the Risk is deemed substantial, re-establish system Integrity before returning to operation;
- If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued Certificates by the CA SHALL be securely notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties;
- If the CA cannot, within fifteen (15) minutes of corruption of computing resources, software, and/or data, correctly reflect the status of Certificates issued by the CA, then all CAs that have been issued Certificates by the CA SHALL be securely notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties; and
- If the ability to Revoke Certificates is inoperative or damaged, the CA SHALL re-establish Revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If the CA's Revocation capability cannot be established in the time-frame specified in the CPS, the CA SHALL determine whether to request Revocation of its Certificate(s). If the CA is the PCA, the CA SHALL determine whether to notify all Subscribers using the CA as a Trust Anchor to delete the Trust Anchor.

5.7.3 Entity (CA) Private Key Compromise Procedures

If a CA's Private Keys are Compromised, lost, or suspected of Compromise, the CA SHALL:

- Notify the MA, PA and (if applicable) ICA PA immediately;
- Generate new keys;
- If the CA can obtain accurate information on the Certificates it has issued and that are still valid (i.e., not expired or Revoked), the CA MAY re-issue (i.e., Renew) those Certificates with the *notAfter* date in the Certificates remaining the same as in original Certificates; and
- If the CA is the PCA, it SHALL provide all Subscribers with the new Trust Anchor using secure means.

The CPS SHALL specify the maximum time during which these procedures MUST be completed.

5.7.3.1 PCA Compromise Procedures

In the case of the PCA Compromise, the CA SHALL notify the MA, PA, Relying Parties, and any cross-certified PKIs, of the PCA Compromise so that they MAY Revoke any Cross-Certificates issued to the PCA or any ICAs and notify all Subscribers and Relying Parties to remove the trusted self-signed Certificate from their trust stores. Notification SHALL be made in an Authenticated and trusted manner. Initiation of notification to the MA and PA and any cross-certified PKIs SHALL be made at the earliest feasible time, which SHALL NOT be longer than the time specified in the CPS, beyond the determination of Compromise or loss unless otherwise required by law enforcement. Initiation of notification to Relying Parties and Subscribers MAY be made after mediations are in place to ensure continued operation of applications and services. If

the cause of the Compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, the CA SHALL then generate a new PCA Certificate, solicit requests and issue new ICA Certificates, securely distribute the new PCA Certificate, and re-establish any Cross-Certificates.

5.7.3.2 Intermediate CA Compromise Procedures

In the event of an ICA key Compromise, the issuing CA SHALL notify the MA, PA, ICA PA (if applicable), and any lower level ICAs. The issuing CA SHALL Revoke the Compromised CA's Certificate, and the Revocation information SHALL be published immediately in the most expedient, Authenticated, and trusted manner after the notification. The Compromised CA SHALL also investigate and report to the MA, PA, ICA PA (if applicable) and any lower level ICAs what caused the Compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the Compromise can be adequately addressed and it is determined that the CA can be securely re-established, then, the CA SHALL be re-established. Upon re-establishment of the CA, new Subscriber Certificates SHALL be requested and issued.

For ICAs, when a Subscriber Certificate is Revoked because of Compromise, suspected Compromise, or loss of the Private Key, a Revocation notice as specified in Section 4.9, SHALL be published at the earliest feasible time by the supporting CA after notification.

5.7.3.3 CSS Compromise Procedures

In case of a CSS key Compromise, the CA that issued the CSS a Certificate SHALL Revoke that Certificate, and the Revocation information SHALL be published immediately in the most expedient, Authenticated, and trusted manner. The CSS SHALL subsequently be Re-Keyed. If the CSS is self-signed and the CSS Certificate expiration is more than twenty-four (24) hours away, the CA SHALL immediately notify the MA, PA, Relying Parties, and any cross-certified PKIs of the CSS Compromise so that they can notify all Subscribers and Relying Parties to remove trust in the CSS Certificate from each Relying Party application, and install the Re-Keyed Certificate.

5.7.3.4 RA Compromise Procedures

In case of a RA Compromise, the CA SHALL disable the RA. In the case that a RA's key is Compromised, the CA that issued the RA Certificate SHALL Revoke it, and the Revocation information SHALL be published in the most expedient, Authenticated, and trusted manner. The Compromise SHALL be investigated by the CA in order to determine the actual or potential date and scope of the RA Compromise. All Certificates approved by that RA since the date of actual or potential RA Compromise SHALL be Revoked. In the event that the scope is indeterminate, then the CA Compromise procedures in Section 5.7.3.2 SHALL be followed.

5.7.4 Business Continuity Capabilities after a Disaster

The CA and RA SHALL develop, test, and maintain a DRP designed to mitigate the effects of any kind of natural or man-made disaster. The DRP SHALL identify conditions for activating the recovery and what constitutes an acceptable system outage and

recovery time for the restoration of Information Systems services and key business functions within a defined recovery time. The CA SHALL provide an alternate secure facility that conforms to all the provisions of the present document for resumption of the CA following any CA service interruption.

CAs SHALL have the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance;
- Certificate Revocation;
- Publication of Revocation information; and
- CA Private Key Compromise.

The disaster recovery equipment SHALL have physical security protections comparable to the production CA system.

The CA SHALL have the ability to fully test its abilities under this section. The CPS SHALL specify a minimum time period where this capability SHALL be demonstrated.

5.8 CA or RA Termination

When a CA operating under this CP terminates operations before all Certificates have expired, entities SHALL be given as much advance notice as circumstances permit.

Prior to CA termination, and in coordination with the MA, the CA SHALL:

- Provide notice to all cross-certified CAs and request Revocation of all Certificates issued to it;
- Issue a CRL revoking all unexpired Certificates prior to termination. This CRL SHALL be available until all Certificates issued by the CA expire;
- Archive all Audit logs and other Records prior to termination;
- Destroy all Private Keys upon termination;
- Archive Records SHALL be transferred to an appropriate authority specified in the CPS; and
- If the PCA is terminated, use secure means to notify the Subscribers to delete all Trust Anchors representing the terminated CA.

Before terminating RA activities, the RA SHALL:

- Provide notice and information about the termination by sending notice by email to Subscribers, Relying Parties, and cross-certifying entities and by posting such information on its web site; and
- Transfer all responsibilities to a successor designated by the MA.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CAs SHALL generate Key Pairs using at a minimum the [FIPS 140-2](#) Level described in Table 6 for the hardware Cryptographic Modules and Key Pair generation processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, Modification, or unauthorized use of Private Keys.

Table 6: Key Pair Generation

Entity	Minimum FIPS 140-2 Level	Hardware Or Software	Key Storage Restricted to the Module on Which the Key was Generated
PCA	3	Hardware	Yes
ICA	3	Hardware	Yes
CSS	2 or higher	Hardware	Yes
End-Entity	1 or higher	Hardware or Software	No stipulation

6.1.1.1 CA Key Pair Generation

CAs SHALL generate CA Key Pairs in a Key Generation Ceremony, using multi-person control, and HSMs validated to the minimum FIPS level specified above. The CA's Key Pair generation MUST create a verifiable Audit trail demonstrating that the security requirements for the procedure was followed. The CA's documentation of the procedure MUST show that appropriate role separation was used. A witness SHALL validate the execution of the key generation procedures by witnessing the key generation and examining the signed and documented Record of the key generation.

6.1.1.2 Subscriber Key Pair Generation

Subscribers SHALL perform Key Pair generation by using a FIPS-approved method or equivalent international standard and either a validated hardware or software Cryptographic Module, as shown in Table 6. Subscribers SHALL generate the random numbers and parameters used for key generation material by a FIPS-approved method or equivalent international standard.

6.1.1.3 CSS Key Pair Generation

CAs SHALL generate the cryptographic keying material used by CSSs to sign CRLs or OCSP status information in [FIPS 140-2](#) Level 2 (or higher) validated Cryptographic Modules.

6.1.2 Private Key Delivery to Subscribers

Subscribers SHALL generate their own Key Pairs, so there is no stipulation for delivering Private Keys to Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber SHALL deliver the Public Key to the RA in a PKCS #10 CSR file, or an equivalent method ensuring that the Public Key has not been altered during transit. The RA SHALL verify the Subscriber's identity and Authenticate the delivery of the Subscriber's Public Key to the RA. The RA Authenticates to the CA's Certificate issuance portal and sends the Public Key CSR file to the CA to request a Certificate on behalf of the Subscriber.

6.1.4 CA Public Key Delivery to Relying Parties

The CA SHALL provide their CA Public Key Certificate to Relying Parties in a secure manner to preclude substitution attacks. Acceptable methods for secure delivery are:

- Secure distribution of CA Certificates through secure Out-of-Band mechanisms; and
- Downloading the CA Certificate from trusted websites.

6.1.5 Key Sizes

Key Pairs SHALL be of sufficient length to prevent others from determining the Key Pair's Private Key using cryptanalysis during the period of expected utilization of such Key Pairs.

PCA Certificates SHALL meet or exceed the following requirements for key size:

Table 7: Key Sizes

Certificate	Key Size
PCA Certificate	4096 – bit RSA
ICA Certificate	3072 – bit RSA
CSS Certificate	At least 2048 – bit RSA
Authentication Certificate (Agency, Element, User)	At least 2048 – bit RSA
Signing Certificate	256 – bit ECC

6.1.6 Public Key Parameters Generation and Quality Checking

Public Key parameters SHALL always be generated and validated in accordance with [FIPS 186-4](#). RAs SHALL only use CSRs containing a Public Key that meets the required key sizes for the requested Certificate.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the *keyUsage* extension in the X.509 Certificate.

The extended key usage SHALL meet the requirements stated in Section 7.1.2. *extKeyUsage* OIDs SHALL be consistent with *keyUsage* bits asserted.

6.1.7.1 *keyUsage* Extension for CA Certificates

Table 8 shows the specific *keyUsage* extension settings for CA Certificates (i.e., the PCA and ICAs) and specifies that all CA Certificates:

- SHALL include a *keyUsage* extension;
- SHALL set the criticality of the *keyUsage* extension to TRUE;
- SHALL assert the *digitalSignature* bit if the CA signs OCSP responses;
- SHALL assert the *keyCertSign* bit; and
- SHALL assert the *cRLSign* bit.

Table 8: *keyUsage* Extension for all CA Certificates

Field	Format	Criticality	Value	Comment
<i>keyUsage</i>	BIT STRING	TRUE	{ id-ce 15 }	Included in all CA Certificates
<i>digitalSignature</i>	(0)		1	Set if the CA signs OCSP responses
<i>nonRepudiation</i>	(1)		0	Not Set
<i>keyEncipherment</i>	(2)		0	Not Set
<i>dataEncipherment</i>	(3)		0	Not Set
<i>keyAgreement</i>	(4)		0	Not Set
<i>keyCertSign</i>	(5)		1	Set
<i>cRLSign</i>	(6)		1	Set
<i>encipherOnly</i>	(7)		0	Not Set
<i>decipherOnly</i>	(8)		0	Not Set

6.1.7.2 *keyUsage* Extension for all End-Entity Certificates

Table 9 shows the specific *keyUsage* extension settings for Agency and Agent Certificates and specifies that all Agency and Agent Certificates:

- SHALL include a *keyUsage* extension;
- SHALL set the criticality to TRUE; and
- SHALL set the *digitalSignature* and *nonRepudiation* bits.

Table 9: *keyUsage* Extension for all Agency and Agent Certificates

Field	Format	Criticality	Value	Comment
<i>keyUsage</i>	BIT STRING	TRUE	{ id-ce 15 }	Included in all Agency and Agent Certificates
<i>digitalSignature</i>	(0)		1	Set
<i>nonRepudiation</i>	(1)		1	Set

Table 10 shows the specific *keyUsage* extension settings for Element Certificates and specifies that all Element Certificates:

- SHALL include a *keyUsage* extension;
- SHALL set the criticality to TRUE; and
- SHALL set the *digitalSignature* and *keyEncipherment* bits.

Table 10: *keyUsage* Extension for all Element Certificates

Field	Format	Criticality	Value	Comment
<i>keyUsage</i>	BIT STRING	TRUE	{ id-ce 15 }	Included in all Element Certificates
<i>digitalSignature</i>	(0)		1	Set
<i>keyEncipherment</i>	(2)		1	Set

Table 11 shows the specific *keyUsage* extension settings for Signing Certificates and specifies that all Signing Certificates:

- SHALL include a *keyUsage* extension;
- SHALL set the criticality to TRUE; and
- SHALL set the *digitalSignature* bit.

Table 11: *keyUsage* Extension for all Signing Certificates

Field	Format	Criticality	Value	Comment
<i>keyUsage</i>	BIT STRING	TRUE	{ id-ce 15 }	Included in all Signing Certificates
<i>digitalSignature</i>	(0)		1	Set

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private Key holders SHALL take necessary precautions to prevent the loss, disclosure, Modification, or unauthorized use of such Private Keys in accordance with this section of the CP.

6.2.1 Cryptographic Module Standards and Controls

Table 6, in Section 6.1.1, summarizes the minimum requirements for Cryptographic Modules; higher levels MAY be used. In addition, Private Keys SHALL NOT exist outside the Cryptographic Module in plaintext form.

6.2.2 Private Key (n out of m) Multi-Person Control

A single person SHALL NOT be permitted to activate or Access any Cryptographic Module that contains the complete CA Private Key. CA Private Keys SHALL be backed up only under multi-person control. Access to CA Private Keys backed up for disaster recovery SHALL be under multi-person control.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Keys

The CA Private Keys SHALL be transported and backed up under the same multi-person control as the original Private Key. At least one (1) copy of the Private Key SHALL be stored off-site. All copies of the CA Private Key SHALL be accounted for and protected in the same manner as the original.

6.2.4.2 Backup of Subscriber Private Keys

Subscriber Private Keys MAY be backed up or copied, but SHALL be held under the control of the Subscriber or other authorized administrator. Subscriber backed up Private Keys SHALL NOT be stored in plaintext format outside the Cryptographic Module. Storage SHALL ensure security controls consistent with the protection provided by the Certificate's Cryptographic Module.

6.2.5 Private Key Archival

The PCA, ICAs, and Subscribers SHALL NOT Archive Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

PCA and ICA Private Keys MAY be exported from the Cryptographic Module only to perform CA key Backup procedures as described in Section 6.2.4.1. At no time SHALL the CA Private Key exist in plaintext form outside the Cryptographic Module.

In the event that a Private Key is to be transported from one Cryptographic Module to another, the Private Key MUST be encrypted during transport; Private Keys MUST NEVER exist in plaintext form outside the Cryptographic Module boundary.

Private or symmetric keys used to encrypt other Private Keys for transport SHALL be protected from disclosure.

Entry of a Private Key into a Cryptographic Module SHALL use mechanisms to prevent loss, theft, Modification, unauthorized disclosure, or unauthorized use of such Private Key.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in [FIPS 140-2](#) (or equivalent standard).

6.2.8 Method of Activating Private Key

Subscribers MUST be Authenticated to the Cryptographic Module before the activation of their associated Private Key(s). Acceptable means of Authentication include, but are not limited to, passphrases, PINs, or Biometrics. Entry of Activation Data SHALL be protected from disclosure (i.e., the data SHOULD NOT be displayed while it is entered).

A device MAY be configured to activate its Private Key without requiring Activation Data, provided that appropriate physical and logical Access Controls are implemented for the device and its Cryptographic Module. The Device's PKI Sponsor SHALL be responsible for ensuring that the system has security controls commensurate with the level of Threat in the device's environment. These controls SHALL protect the device's hardware, software, and the cryptographic token and its Activation Data from Compromise.

The PCA and all ICAs SHALL protect the Activation Data for their Private Keys against loss, theft, Modification, disclosure, or unauthorized use.

6.2.8.1 CA Administrator Activation

Method of activating the CA system by a CA Administrator SHALL require:

- Use of a smart card, Biometric Access device, and/or password in accordance with Section 6.4.1, or security of equivalent strength to Authenticate the CA Administrator before the activation of the Private Key; and
- Commercially reasonable measures for the physical protection of the CA Administrator's workstation to prevent use of the workstation and its associated Private Key without the CA Administrator's authorization.

6.2.8.2 Offline CAs Private Key

Once the CA system has been activated, a threshold number of Multi-Person Private Key holders SHALL be REQUIRED to supply their Activation Data in order to activate an offline CA's Private Key, as defined in Section 6.2.2. Once the Private Key is activated, it SHALL only be active until termination of the session.

6.2.8.3 Online CAs Private Keys

An online CA's Private Key SHALL be activated by a threshold number of Multi-Person Private Key holders, as defined in Section 6.2.2, supplying their Activation Data (stored on secure media). Once the Private Key is activated, the Private Key MAY be active for an indefinite period until it is deactivated when the CA goes offline.

6.2.9 Method of Deactivating Private Key

After use, Private Key holders SHALL deactivate the Cryptographic Module, e.g., via a manual logout procedure or automatically after a period of inactivity. When deactivated, Private Keys SHALL be kept in encrypted form only. Private Keys SHALL be cleared from memory before the memory is de-allocated. Any disk space where Private Keys were stored SHALL be overwritten before the space is released to the operating system. CA and CSS Cryptographic Modules SHALL be stored in a secure container when not in use.

6.2.10 Method of Destroying Private Key

Private Key holders SHALL destroy their Private Keys when they are no longer needed or when the Certificates to which they correspond expire or are Revoked. Physical destruction of hardware is not required.

CA Private Key destruction procedures SHALL be sufficient to ensure that it is impossible to recover any part of the Private Key from any Cryptographic Module, memory or disk space.

If proper destruction of a Private Key cannot be guaranteed, then the key SHALL be treated as Compromised and its corresponding Public Key Certificate Revoked.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The Public Key is Archived as part of the Certificate archival described in Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The usage period for the PCA Key Pair is a maximum ten (10) years. For ICAs operating under this CP, the usage period for a CA Key Pair is a maximum of three (3) years. The CA Private Key MAY be used to sign Certificates for at most three (3) years, but MAY be used to sign CRLs and Certificates for the entire usage period.

To minimize Risk from Compromise of a CA's Private Key, that key MAY be changed often; from that time on, only the new key SHALL be used for Certificate signing purposes. The older, but still valid, Certificate will be available to verify old signatures until all the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign OCSP responder Certificates or CRLs, then the old key SHALL be retained and protected.

When a CA updates its Private Key and thus generates a new Public Key, the CA SHALL notify all CAs and Subscribers that rely on the CA's Certificate that it has been changed.

Table 12 provides the lifetimes for the Private Keys and Certificates issued to the owner of that Private Key.

Table 12: Certificate Validity Periods

Certificate	Certificate Validity	Key Validity Period
PCA	Up to 10 Years	10 years
Intermediate CA	Up to 3 Years	3 years
Authentication Certificates	Up to 3 Years	3 years
Signing Certificates	Up to 3 Years	10 years*

** The Key Pair for Signing Certificates cannot be reused after the initial Certificate Validity Period, but the Private Key MAY be escrowed for up to ten (10) years.*

Validity Periods SHALL be nested such that the Validity Periods of issued Certificates SHALL be contained within the Validity Period of the issuing CA. In other words, CAs SHALL NOT issue Certificates that extend beyond the expiration date of their own

Certificates and Public Keys. All Certificates signed by a specific CA Key Pair MUST expire before the end of that Key Pair's usage period. There is a difference between the Certificate Validity Period and the Key Validity Period. The Validity Period of the Certificate indicates a period for which the Public Key bound to the Certificate MAY be used. The key Validity Period indicates the usage period for the Private Key, which is dependent on key size and usage.

ICA CPSs SHOULD NOT allow End-Entity Certificates to have a Validity Period of over one (1) year, and SHOULD limit End-Entity Certificate validity to no more than three (3) months. Where an ICA CPS provides for End-Entity Certificates that are valid for more than one (1) year, the CPS SHALL justify the purposes for a longer Validity Period.

PCA PKI Participants SHALL cease all use of their Private Key Pairs after their Validity Period has expired.

Notwithstanding the above table, in all cases the CA Private Key MAY be used to sign OCSP responder Certificates (if applicable) and CRLs until the CA Certificate expires.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Private Key holders SHALL use Activation Data to unlock Private Keys, in conjunction with any other Access Control, which have an appropriate level of strength for the keys or data to be protected and SHALL meet the applicable Security Policy requirements of the Cryptographic Module used to store the keys. Two (2)-factor Authentication SHALL be used to Authenticate users prior to unlocking Private Keys. To the extent passwords are used as Activation Data, the PCA's and ICAs' activation participants SHALL generate passwords that cannot easily be guessed or cracked. Participants MAY NOT need to generate Activation Data, for example, if they use Biometric Access devices.

CAs SHALL either entail the use of Biometric data or satisfy the policy-enforced at/by the Cryptographic Module. If the CA MUST transmit Activation Data, it SHALL be via an appropriate protected channel, and distinct in time and place from the associated Cryptographic Module. The CA SHALL change its Activation Data upon CA Re-Key.

RA and Subscriber Activation Data MAY be user-selected. The strength of the Activation Data SHALL meet or exceed the requirements for Authentication mechanisms stipulated for Level 1 or higher in [FIPS 140-2](#), or some other equivalent standard. If the Activation Data MUST be transmitted, it SHALL be via an appropriately protected channel, and distinct in time and place from the associated Cryptographic Module.

6.4.2 Activation Data Protection

Private Key holder Activation Data used to unlock Private Keys SHALL be protected from disclosure by a combination of cryptographic and physical Access Control mechanisms, such as:

- Memorization;
- Biometric in nature; or

- Recorded and secured at the level of assurance associated with the activation of the Cryptographic Module, and SHALL NOT be stored with the Cryptographic Module.

In all cases, the protection mechanism implemented by Private Key holders SHALL include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CA computer security functions SHALL:

- Require Authenticated logins;
- Require users to select strong passwords;
- Provide Security Audit capability;
- Lock the Access to CA services after a determined amount of unsuccessful login attempts;
- Restrict Access Control to CA services;
- Enforce separation of duties for Trusted Roles;
- Require identification and Authentication of Trusted Roles;
- Archive history and Audit Data;
- Employ malicious code protection mechanisms to mitigate the Risk of malicious code on CA system components;
- Employ technical and procedural controls to prevent and detect unauthorized changes to firmware and software on CA systems;
- Require Backups for recovery of keys and the CA system; and
- Enforce domain Integrity boundaries for security critical CA processes.

RA computer security functions SHALL:

- Require Authenticated logins;
- Require users to select strong passwords;
- Provide Security Audit capability;
- Lock Access to RA services after a determined amount of unsuccessful login attempts;
- Restrict Access Control to RA services;
- Enforce separation of duties for Trusted Roles;
- Require identification and Authentication of Trusted Roles; and
- Archive history and Audit Data.

The CA and RA functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

All communications between any PKI Trusted Role and the CA MUST be Authenticated and protected from Modification.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls address various aspects related to the development and change of the PCA and ICA systems through aspects of its life-cycle. The system development controls for CAs SHALL:

- Use software that has been designed and developed under a formal, documented development methodology;
- Procure hardware and software in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Develop hardware and software in a controlled and documented environment to demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment;
- Deliver all hardware and software via controlled methods that provide a continuous chain of accountability from the purchase location to the operations location;
- Dedicate hardware and software to performing PKI activities;
- Prevent malicious software from being loaded onto the equipment by implementing and testing in a non-production environment prior to implementation in a production environment;
- Obtain applications required to perform PKI operations from sources authorized by local policy;
- Scan CA hardware and software for malicious code on first use and periodically thereafter; and
- Purchase or develop hardware and software updates in the same manner as original equipment, and installed using trusted and trained personnel.

6.6.2 Security Management Controls

A list of acceptable products and their versions for each individual PCA and ICA system component SHALL be maintained and kept up-to-date within a configuration management system.

To reduce the available attack surface of a CA system, only those ports, protocols, and services that are necessary to the CA system architecture are permitted to be installed or operating. The CA system SHALL maintain a list of ports, protocols, and services that are necessary for the correct function of each component within the CA system.

The configuration of the CA system, in addition to any modifications and upgrades, SHALL be documented and controlled. The CA software, when first loaded, SHALL be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

The CA system SHALL provide a mechanism to periodically verify the Integrity of the software.

The CA SHALL also have mechanisms and policies in place to control and monitor the configuration of the CA system.

6.6.3 Life Cycle Security Controls

The PCA and ICAs SHALL have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption. A log SHALL be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches.

From time to time, the CA MAY discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The CA SHALL correct such errors and document the reason for the error, and the associated correction. In the event a vulnerability is detected with a rated severity value of nine (9) or higher on the US-CERT CVSS 3.1 [\[CVSS\]](#) rating scale, remediation SHALL be effected within forty-five (45) days after patch availability.

Remediation activities SHOULD NOT cause unavailability of Revocation information.

6.7 Network Security Controls

Many components of a CA are connected to each other and their customers via various forms of networks. While it is necessary for connections to customers and administrative systems, care needs to be taken to ensure those connections do not adversely impact the security of those components. Guidelines for effective CA networking security are discussed in the following sections.

The CPS SHALL describe how network security is configured and validated.

6.7.1 Isolation of Networked Systems

The PCA and its Private Keys SHALL be offline.

Communication channels between the network-connected ICA components and the trusted CA processing components SHALL be protected against attack. Furthermore, information flowing into these CA components from the network-connected CA components SHALL NOT lead to any Compromise or disruption of these components.

The components of a CA requiring direct network connections SHALL be minimized. Those networked components SHALL be protected from attacks by adequate means to filter unwanted protocols (utilizing Access rules, whitelists, blacklists, protocol checkers, etc., as necessary). Data loss prevention tools SHALL be employed to detect

inappropriate leakage of sensitive information. Such components SHOULD be secure without the use of a Firewall.

6.7.2 Boundary Protection

Any boundary control devices used to protect a CA's Repository or CA's local area network SHALL deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

The PCA and ICAs, the RAs on their behalf, Repositories, remote workstations used to administer the CAs, and CSS SHALL employ appropriate network security controls. Networking equipment SHALL turn off unused network ports and services. Any network software present SHALL be necessary to the functioning of the equipment.

6.7.2.1 Transmission Confidentiality

Intra-CA communications that cross the physical protection barrier of the Certificate signing portion of a CA system SHALL protect the Confidentiality. Services used by a CA system that are not administered by its CA Administrator SHALL provide protection commensurate with this CP.

Confidentiality of Subscriber data SHALL be maintained as negotiated between the RA and the Subscriber or the Subscriber's organization.

6.7.3 Network Monitoring

The CA SHALL monitor the CA system to detect attacks and indicators of potential attacks.

6.8 Time-Stamping

Certificates, CRLs, and other Revocation database entries SHALL contain time and date information.

Asserted times SHALL be accurate to within 100ms. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are Auditable events (see Section 5.4.1).

All CA components SHALL regularly synchronize with a time service such as National Institute of Standards and Technology (NIST) Atomic Clock or NIST Network Time Protocol Service, a master clock it operates, or is operated by a public safety entity. Time derived from the time service SHALL be used for establishing the time of:

- Initial validity type of a Certificate;
- Revocation of a Certificate;
- Posting of CRL updates; and
- OCSP responses.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates issued by a CA under this CP SHALL conform to [RFC 5280](#) Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008.

CA Certificates SHALL contain the identity and attribute data of a Subject using the base Certificate with applicable extensions. The base Certificate SHALL contain the version number of the Certificate, the Certificate's identifying serial number, the signature algorithm used to sign the Certificate, the issuer's DN, the Validity Period of the Certificate, the Subject's DN, information about the Subject's Public Key, and extensions (See Table 13).

Table 13: Certificate Profile Basic Fields

Field	[RFC 5280] Section	Requirement or Recommendation
<i>tbsCertificate</i>	4.1.1.1	Follows RFC 5280 guidance
<i>version</i>	4.1.2.1	See CP Section 7.1.1.
<i>serialNumber</i>	4.1.2.2	SHALL be a unique positive integer assigned by the CA and SHALL NOT be longer than 20 octets.
<i>signature</i>	4.1.2.3	See CP Section 7.1.3.
<i>issuer</i>	4.1.2.4	See CP Section 3.1.1.
<i>validity</i>	4.1.2.5	See CP Section 6.3.2.
<i>subject</i>	4.1.2.6	See CP Section 7.1.4.
<i>subjectPublicKeyInfo</i>	4.1.2.7	See CP Section 7.1.3.
<i>extensions</i>	4.1.2.9	See CP Section 7.1.2.
<i>signatureAlgorithm</i>	4.1.1.2	Follows RFC 5280 guidance
<i>algorithmIdentifier</i>	4.1.1.2	See CP Section 7.1.3.
<i>algorithm</i>	4.1.1.2	See CP Section 7.1.3.
<i>parameters</i>	4.1.1.2	See CP Section 7.1.3.
<i>signatureValue</i>	4.1.1.3	Follows RFC 5280 guidance

7.1.1 Certificate Version Number(s)

The PCA and ICAs SHALL issue X.509 v3 Certificates. The CA SHALL set the Certificate version number to the integer value of "2" to designate a version 3 Certificate.

7.1.2 Certificate Extensions

CA Certificate extensions provide methods for associating additional attributes with Public Keys and for managing relationships between CAs. CA Certificates SHALL follow

the guidance in [RFC 5280](#) and SHALL contain the standard extensions shown in the tables below, unless they are denoted as optional.

7.1.2.1 Standard Extension for PCA Certificates

Table 14 shows the Certificate extensions for all PCA Certificates.

Table 14: PCA Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
<i>basicConstraints</i>	[RFC 5280]	4.2.1.9	SHALL be included in PCA Certificate. Criticality SHALL be set to TRUE.
<i>keyUsage</i>	[RFC 5280]	4.2.1.3	SHALL be included in PCA Certificate. Criticality SHALL be set to TRUE.
<i>subjectAltName</i>	[RFC 5280]	4.2.1.6	MAY be included in PCA Certificate. Criticality SHALL be set to FALSE.
<i>subjectKeyIdentifier</i>	[RFC 5280]	4.2.1.2	SHALL be included in PCA Certificate. Criticality SHALL be set to FALSE.

7.1.2.2 Standard Extension for ICA Certificates

Table 15 shows the Certificate extensions for all ICA Certificates.

Table 15: ICA Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
<i>authorityInformationAccess</i>	[RFC 5280]	4.2.2.1	SHALL be included in ICA Certificates. Criticality SHALL be set to FALSE.
<i>authorityKeyIdentifier</i>	[RFC 5280]	4.2.1.1	SHALL be included in ICA Certificates. Criticality SHALL be set to FALSE.
<i>basicConstraints</i>	[RFC 5280]	4.2.1.9	SHALL be included in ICA Certificates. Criticality SHALL be set to TRUE.
<i>certificatePolicies</i>	[RFC 5280]	4.2.1.4	MAY be included in ICA Certificates. Criticality SHALL be set to FALSE.
<i>crlDistributionPoints</i>	[RFC 5280]	4.2.1.13	SHALL be included in all ICA Certificates. Criticality SHALL be set to FALSE.
<i>keyUsage</i>	[RFC 5280]	4.2.1.3	SHALL be included in ICA Certificates. Criticality SHALL be set to TRUE.
<i>subjectAltName</i>	[RFC 5280]	4.2.1.6	MAY be included in ICA Certificates. Criticality SHALL be set to FALSE.
<i>subjectInformationAccess</i>	[RFC 5280]	4.2.2.2	SHALL be included in ICA Certificates with non-zero <i>pathLenConstraints</i> . Criticality SHALL be set to FALSE.
<i>subjectKeyIdentifier</i>	[RFC 5280]	4.2.1.2	SHALL be included in ICA Certificates. Criticality SHALL be set to FALSE.

7.1.2.3 Standard Extensions for End-Entity Certificates

Table 16 shows the Certificate extensions for all End-Entity Certificates.

Table 16: End-Entity Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
<i>authorityInformationAccess</i>	[RFC 5280]	4.2.2.1	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
<i>authorityKeyIdentifier</i>	[RFC 5280]	4.2.1.1	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
<i>certificatePolicies</i>	[RFC 5280]	4.2.1.4	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
<i>crlDistributionPoints</i>	[RFC 5280]	4.2.1.13	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
<i>extKeyUsage</i>	[RFC 5280]	4.2.1.12	SHALL be included in Element and Signing Certificates. SHALL NOT be included in Agency or Agent Certificates. If included, then criticality SHALL be set to TRUE in End-Entity Certificates.
<i>keyUsage</i>	[RFC 5280]	4.2.1.3	SHALL be included in End-Entity Certificates. Criticality SHALL be set to TRUE.
<i>subjectAltName</i>	[RFC 5280]	4.2.1.6	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
<i>subjectKeyIdentifier</i>	[RFC 5280]	4.2.1.2	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.

7.1.2.4 Authority Information Access Extension

The *authorityInformationAccess* (or *authorityInfoAccess*) extension indicates how to Access OCSP information for the Certificate issuer.

Table 17 shows the *authorityInfoAccess* extension settings for ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *authorityInfoAccess* extension;
- SHALL set the criticality of the *authorityInfoAccess* extension to FALSE;
- SHALL set the *accessMethod* OID to 1.3.6.1.5.5.7.48.1 for OCSP; and
- SHALL set the *accessLocation* to the URL of the OCSP responder.

Table 17: *authorityInfoAccess* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
<i>authorityInfoAccess</i>		FALSE	{ id-pe 1 }	Included in all ICA Certificates.
<i>accessMethod</i>	OID		1.3.6.1.5.5.7.48.1	OCSP {id-pkix-ocsp}
<i>accessLocation</i>	General Name		URL	Address of the OCSP responder

Table 18 shows the *authorityInfoAccess* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- SHALL include the *authorityInfoAccess* extension;
- SHALL set the criticality of the *authorityInfoAccess* extension to FALSE;
- SHALL set the *accessMethod* OID to 1.3.6.1.5.5.7.48.2 for *cAIssuer*;
- SHALL set the *accessLocation* to the URL of the CA Issuer Certificate;
- SHALL set the *accessMethod* OID to 1.3.6.1.5.5.7.48.1 for OCSP; and
- SHALL set the *accessLocation* to the URL of the OCSP responder.

Table 18: *authorityInfoAccess* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
<i>authorityInfoAccess</i>		FALSE	{ id-pe 1 }	Included in all End-Entity Certificates.
<i>accessMethod</i>	OID		1.3.6.1.5.5.7.48.2	<i>cAIssuer</i>
<i>accessLocation</i>			URL	Location of CA Issuer Certificate
<i>accessMethod</i>	OID		1.3.6.1.5.5.7.48.1	OCSP {id-pkix-ocsp}
<i>accessLocation</i>	General Name		URL	Address of the OCSP responder

7.1.2.5 Authority Key Identifier Extension

The *authorityKeyIdentifier* extension provides a means to identify the identity of the Public Key corresponding to the Private Key used to sign a Certificate.

Table 19 shows the *authorityKeyIdentifier* extension settings for ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *authorityKeyIdentifier* extension;
- SHALL set the criticality of the *authorityKeyIdentifier* extension to FALSE; and
- SHALL calculate the *keyIdentifier* of the *authorityKeyIdentifier* per Method 1.

Table 19: *authorityKeyIdentifier* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
<i>authorityKeyIdentifier</i>		FALSE	{ id-ce 35 }	Included in all ICA Certificates.
<i>keyIdentifier</i>	OCTET STRING		< <i>keyIdentifier</i> >	Calculated per Method 1

Table 20 shows the *authorityKeyIdentifier* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- SHALL include the *authorityKeyIdentifier* extension;
- SHALL set the criticality of the *authorityKeyIdentifier* extension to FALSE; and
- SHALL calculate the *keyIdentifier* of the *authorityKeyIdentifier* per Method 1.

Table 20: *authorityKeyIdentifier* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
<i>authorityKeyIdentifier</i>		FALSE	{ id-ce 35 }	Included in all End-Entity Certificates.
<i>keyIdentifier</i>	OCTET STRING		< <i>keyIdentifier</i> >	Calculated per Method 1

7.1.2.6 Basic Constraints Extension

The *basicConstraints* extension identifies whether the Subject of a Certificate is a CA and the maximum depth of valid certification paths that include the Certificate.

NOTE: The *pathLenConstraint* field gives the maximum number of ICA Certificates that MAY follow this Certificate in the certification path. A value of "0" indicates that only an End-Entity Certificate MAY follow in the path. If the *pathLenConstraint* value is set, it has to be greater than or equal to zero (0). If it is not set, then the certification path MAY be of any length.

Table 21 shows the *basicConstraints* extension settings for Root CA Certificates (for example, the PCA) and specifies that all Root CA Certificates:

- SHALL include the *basicConstraints* extension;
- SHALL set the criticality of the *basicConstraints* extension to TRUE;
- SHALL set the cA field of the *basicConstraints*; and
- SHALL set the *pathLenConstraint* field of the *basicConstraints* to "None".

Table 21: *basicConstraints* Extension for Root CA Certificates

Field	Format	Criticality	Value	Comment
<i>basicConstraints</i>		TRUE	{ id-ce 19 }	Included in all Root CA Certificates.
<i>cA</i>	BOOLEAN		TRUE	Set
<i>pathLenConstraint</i>	INTEGER		None	Not Set

Table 22 shows the *basicConstraints* extension settings for Tier-2 ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *basicConstraints* extension;
- SHALL set the criticality of the *basicConstraints* extension to TRUE;
- SHALL set the *cA* field of the *basicConstraints*; and
- SHALL set the *pathLenConstraint* field of the *basicConstraints* to "3" for a Tier-2 ICA.

Table 22: *basicConstraints* Extension for Tier-2 ICA Certificates

Field	Format	Criticality	Value	Comment
<i>basicConstraints</i>		TRUE	{ id-ce 19 }	Included in all ICA Certificates.
<i>cA</i>	BOOLEAN		TRUE	Set
<i>pathLenConstraint</i>	INTEGER		3	Set

Table 23 shows the *basicConstraints* extension settings for Tier-3 ("Tier-n") and above (Tier-N) ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *basicConstraints* extension;
- SHALL set the criticality of the *basicConstraints* extension to TRUE;
- SHALL set the *cA* field of the *basicConstraints*; and
- CA SHALL set *pathLenConstraint* field of any ICA Certificate it issues to its own *pathLenConstraint* -1.

Table 23: *basicConstraints* Extension for Tier-n ICA Certificates

Field	Format	Criticality	Value	Comment
<i>basicConstraints</i>		TRUE	{ id-ce 19 }	Included in all ICA Certificates.
<i>cA</i>	BOOLEAN		TRUE	Set
<i>pathLenConstraint</i>	INTEGER		5 – n	Set

7.1.2.7 Certificate Policies Extension

See Section 7.1.6.

7.1.2.8 CRL Distribution Points Extension

The *cRLDistributionPoints* extension identifies how CRL information is obtained.

Table 24: *cRLDistributionPoints* Extension for ICA Certificates shows the *cRLDistributionPoints* extension settings for ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *cRLDistributionPoints* extension;
- SHALL set the criticality of the *cRLDistributionPoints* extension to FALSE; and
- SHALL set the *distributionPointName* to the URL of the CRL.

Table 24: *cRLDistributionPoints* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
<i>cRLDistributionPoints</i>		FALSE	{ id-ce 31 }	Included in all ICA Certificates.
<i>distributionPoint</i>				
<i>distributionPointName</i>	General Names		URL	Address of the CRL

Table 25: *cRLDistributionPoints* Extension for End-Entity Certificates shows the *cRLDistributionPoints* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- SHALL include the *cRLDistributionPoints* extension;
- SHALL set the criticality of the *cRLDistributionPoints* extension to FALSE; and
- SHALL set the *distributionPointName* to the URL of the CRL.

Table 25: *cRLDistributionPoints* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
<i>cRLDistributionPoints</i>		FALSE	{ id-ce 31 }	Included in all End-Entity Certificates.
<i>distributionPoint</i>				
<i>distributionPointName</i>	General Names		URL	Address of the CRL

7.1.2.9 Extended Key Usage Extension

The *extendedKeyUsage* (or *extKeyUsage*) extension indicates one (1) or more purposes for which the Public Key MAY be used, in addition to, or in place of, the purposes indicated in the *keyUsage* extension.

Agency and Agent Certificates SHALL NOT include the *extKeyUsage* extension.

Table 26: *extendedKeyUsage* Extension for Element Certificates shows the *extKeyUsage* extension settings for Element Certificates and specifies that all Element Certificates:

- SHALL include the *extKeyUsage* extension;

- SHALL set the criticality of the *extKeyUsage* extension to TRUE; and
- SHALL set the *keyPurposeId* field to *id-kp-clientAuth* and *id-kp-serverAuth*.

Table 26: *extendedKeyUsage* Extension for Element Certificates

Field	Format	Criticality	Value	Comment
<i>extKeyUsage</i>		TRUE	{ id-ce 37 }	Included in Element Certificates.
<i>keyPurposeId</i>	OID		1.3.6.1.5.5.7.3.1	<i>id-kp-serverAuth</i> Included in Element Certificates
<i>keyPurposeId</i>	OID		1.3.6.1.5.5.7.3.2	<i>id-kp-clientAuth</i> Included in Element Certificates

Table 27: *extendedKeyUsage* Extension for Signing Certificates shows the *extKeyUsage* extension settings for Signing Certificates and specifies that all Signing Certificates:

- SHALL include the *extKeyUsage* extension;
- SHALL set the criticality of the *extKeyUsage* extension to TRUE; and
- SHALL set the *keyPurposeId* field to *id-kp-codeSigning*.

Table 27: *extendedKeyUsage* Extension for Signing Certificates

Field	Format	Criticality	Value	Comment
<i>extKeyUsage</i>		TRUE	{ id-ce 37 }	Included in all Signing Certificates.
<i>keyPurposeId</i>	OID		1.3.6.1.5.5.7.3.3	<i>id-kp-codeSigning</i> Included in Signing Certificates

7.1.2.10 Key Usage Extension

See Section 6.1.7.

7.1.2.11 Subject Alternative Name Extension

The *subjectAlternativeName* (or *subjectAltName*) extension allows identities to be bound to the Subject of the Certificate.

The *otherName* field SHALL include a single quad that includes fields "*idType*", "*iD*", "*role*", and "*owner*" using UTF-8 encoding, delimited by a forward slash. For *idTypes* of *agencyID*, there MAY be no logical owner, so the "Owner" field MAY be null.

The *idType* SHALL include the values as allowed in the [NENA i3](#) standard (e.g., *agentId*, *agencyId*, *elementId*)⁷ or the value "*cAId*" if the Certificate is a CA Certificate.

The *cAId* value for CA Certificates SHALL be an FQDN under the CA owner's control, subject to validation as documented in the [VP](#).

⁷ See NENA i3 at Section 2.1.

The Owner field SHALL contain the *iD* of the issuing Agency. For an ICA, the owner field SHALL contain the *iD* of the issuing CA or the owner Agency.

The whole of the *otherName* field SHALL be globally unique.

Role SHALL include a list of comma delimited roles as defined in the [NENA i3](#) Standard and appropriate registries;⁸ for *cAId*, roles SHALL be one of either "PCA" for the PCA or "ICA" for any ICA. The OID for the quad SHALL be the child OID specified for this quad in 1.2.2.

An example of a valid *otherName* value for an Agency that processes emergency calls and includes a local police, fire and EMS function is below:

OBJECT IDENTIFIER 1.3.6.1.4.1.55670.1.1

[0] (1 elem)

```
UTF8String
agencyId/foo.allegheny.pa.us/urn:emergency:service:responder.psap,
urn:emergency:service:responder.police.local,
urn:emergency:service:responder.fire.local,
urn:emergency:service:responder.ems.local/
```

An example of a valid *otherName* value for an individual (Agent) named John Smith who processes emergency calls and also dispatches resources is below:

OBJECT IDENTIFIER 1.3.6.1.4.1.55670.1.1

[0] (1 elem)

```
UTF8String agentId/jsmith@psap.allegheny.pa.us/Dispatching,CallTaking/
psap.allegheny.pa.us
```

Table 28 shows the *subjectAltName* extension settings for all Root Certificates and specifies that all Root Certificates:

- SHALL include the *subjectAltName* extension;
- SHALL set the criticality of the *subjectAltName* extension to FALSE; and
- SHALL set the *directoryName* with the appropriate information.

⁸ See NENA i3 at Section 5.3

Table 28: *subjectAlternativeName* Extension for Root Certificates

Field	Format	Criticality	Value	Comment
<i>subjectAltName</i>		FALSE	{ id-ce 17 }	SHALL be included in all PCA Certificates.
<i>otherName</i>	OtherName (UTF8 String)		Quad ID OID	Single quad that includes fields " <i>idType</i> ", " <i>iD</i> ", " <i>role</i> ", and " <i>owner</i> " in UTF-8 encoding, delimited by a forward slash

Table 29 shows the *subjectAltName* extension settings for all ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *subjectAltName* extension;
- SHALL set the criticality of the *subjectAltName* extension to FALSE; and
- SHALL set the *otherName* with the appropriate information.

Table 29: *subjectAlternativeName* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
<i>subjectAltName</i>		FALSE	{ id-ce 17 }	SHALL be included in all CA Certificates.
<i>otherName</i>	OtherName (UTF8 String)		Quad ID OID	Single quad that includes fields " <i>idType</i> ", " <i>iD</i> ", " <i>role</i> " and " <i>owner</i> " in UTF-8 encoding, delimited by a forward slash

Table 30 shows the *subjectAltName* extension settings for End-Entity Certificates and specifies that End-Entity Certificates:

- SHALL include the *subjectAltName* extension;
- SHALL set the criticality of the *subjectAltName* extension to FALSE;
- SHALL set the *otherName* with the appropriate information;
- Agency and Element Service Certificates SHALL contain *dNSName* and MAY contain *iPAddress*; and
- Agent and Signing Certificates MAY contain *dNSName* and *iPAddress*.

Table 30: *subjectAlternativeName* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
<i>subjectAltName</i>		FALSE	{ id-ce 17 }	SHALL be included in End-Entity Certificates.
<i>otherName</i>	OtherName (UTF8 String)		Quad ID OID	ID that includes fields " <i>idType</i> ", " <i>iD</i> ", " <i>role</i> ", and if applicable, " <i>owner</i> ", in UTF-8 encoding, delimited by a forward slash
<i>dNSName</i>	IA5String			DNS Name(s) If included, the first DNS Name MUST be the <i>iD</i> . Additional DNS Names can be added – wild card names are not allowed.
<i>iPAddress</i>	OCTET String			IP Address

7.1.2.12 Subject Information Access Extension

The *subjectInformationAccess* (or *subjectInfoAccess*) extension indicates how to Access information and services for the Subject of the Certificate in which the extension appears.

Table 31 shows the *subjectInfoAccess* extension settings for ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *subjectInfoAccess* extension;
- SHALL set the criticality of the *subjectInfoAccess* extension to FALSE;
- SHALL set the *accessMethod* OID to *id-ad-caRepository*, and
- SHALL set the *accessLocation* to the URL of the CA Repository.

Table 31: *subjectInformationAccess* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
<i>subjectInfoAccess</i>		FALSE	{ id-pe 11 }	SHALL be included in ICA Certificates.
<i>accessMethod</i>	OID		id-ad-caRepository	
<i>accessLocation</i>	General Names		URL	URL of the CA Repository

7.1.2.13 Subject Key Identifier Extension

The *subjectKeyIdentifier* extension provides a means of identifying Certificates that contain a particular Public Key.

Table 32 shows the *subjectKeyIdentifier* extension settings for CA Certificates and specifies that all CA Certificates:

- SHALL include the *subjectKeyIdentifier* extension;
- SHALL set the criticality of the *subjectKeyIdentifier* extension to FALSE; and
- SHALL calculate the *keyIdentifier* of the *subjectKeyIdentifier* per Method 1.

Table 32: *subjectKeyIdentifier* Extension for CA Certificates

Field	Format	Criticality	Value	Comment
<i>subjectKeyIdentifier</i>		FALSE	{ id-ce 14 }	SHALL be included in all CA Certificates.
<i>keyIdentifier</i>	OCTET STRING		<key identifier>	Calculated per Method 1

Table 33 shows the *subjectKeyIdentifier* extension settings for End-Entity Certificates, and specifies that all End-Entity Certificates:

- SHALL include the *subjectKeyIdentifier* extension;
- SHALL set the criticality of the *subjectKeyIdentifier* extension to FALSE; and
- SHALL calculate the *keyIdentifier* of the *subjectKeyIdentifier* per Method 1.

Table 33: *subjectKeyIdentifier* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
subjectKeyIdentifier		FALSE	{ id-ce 14 }	Included in all End-Entity Certificates.
keyIdentifier	OCTET STRING		<key identifier>	Calculated per Method 1

7.1.3 Algorithm Object Identifiers (OIDs)

Certificates issued under this CP SHALL use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512withRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-Sha2(3) 2}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-Sha2(3) 3}
ecdsa-with-Sha512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-Sha2(3) 3 ecdsa-with-Sha512(4)}
Ed25519	{iso(1) identified-organization(3) thawte(101) id-Ed25519(112)}

Certificates issued under this CP SHALL use the following OIDs to identify the algorithm associated with the Subject key:

<i>rsaEncryption</i>	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Where the Certificate contains an elliptic curve Public Key, the parameters SHALL be specified as one of the following named curves:

secp256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
secp384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34 }
secp521r1	{iso(1) identified-organization(3) certicom(132) curve(0) 35 }
Ed25519	NULL

7.1.4 Name Forms

The Subject field in Certificates issued under this CP SHALL be populated with an [X.500](#) DN as specified in Section 3.1.1.

The issuer field of Certificates issued under this CP SHALL be populated with a non-empty [X.500](#) DN as specified in Section 3.1.1.

7.1.4.1 PCA

The following naming attributes SHALL be used to populate the PCA Certificate Subject fields issued under this CP:

Table 34: PCA Certificate Subject Fields

Name	Field	Value	Requirement
<i>country</i>	(C=)	<Country Name>	(Optional) MAY contain the two (2)-letter ISO 3166-1 country code for the country in which the PCA's service provider's place of business is located.
<i>organizationName</i>	(O=)	<Organization>	SHALL contain the organization name (or abbreviation thereof), trademark, or other meaningful identifier.
<i>organizationalUnitName</i>	(OU=)	<CA type> CA- <Id#>	SHALL contain the CA type (e.g., PCA) and unique ID, e.g., PCA – 1.
<i>commonName</i>	(CN=)	<Name> CA	SHALL contain a name that accurately identifies the PCA (e.g., Organization Name Root CA).

7.1.4.2 ICAs

All attributes permitted by [RFC 5280](#) MAY be populated in the ICA Certificate Subject fields issued under the CP. The following attributes MUST be populated:

Table 35: ICA Certificate Subject Fields

Name	Field	Value	Requirement
<i>country</i>	[C=]	<Country Name>	[Optional] MAY contain the two (2)-letter ISO 3166-1 country code for the country in which the PCA's service provider's place of business is located.
<i>organizationName</i>	(O=)	<Organization>	SHALL contain the organization name (or abbreviation thereof), trademark, or other meaningful identifier.
<i>organizationalUnitName</i>	(OU=)	<CA type> CA- <Id#>	SHALL contain the CA type (e.g., Intermediate or I) and unique ID, e.g., ICA-1.
<i>localityName</i>	[L=]	<Location>	[Optional] MAY contain additional location information e.g., City.
<i>stateOrProvinceName</i>	[ST=]	<state or province>	[Optional] MAY contain the state or province name.
<i>commonName</i>	(CN=)	<Name> ICA	SHALL contain a name that accurately identifies the ICA (e.g., Organization Name ICA).

7.1.4.3 End-Entity Certificates

The following naming attributes SHALL be used to populate the Subject in End-Entity Certificates issued under this CP:

Table 36: End-Entity Certificate Subject Fields

Name	Field	Value	Requirement
<i>countryName</i>	(C=)	<Country Name>	SHALL be the two (2)-letter ISO 3166-1 country code for the country in which the Subscriber's place of business is located.
<i>organizationName</i>	(O=)	<Organization>	SHALL contain the organization name (not to exceed 64 characters).
<i>localityName</i>	[L=]	<Location>	[Optional] <City>
<i>stateOrProvinceName</i>	[st=]	<state or province>	[Optional] <state or province name>
<i>organizationalUnitName</i>	[OU=]	<subsidiary/location>	[Optional] subsidiary/location (not to exceed 64 characters)

<i>commonName</i>	[CN=]	<ID of the Quad ID >	[Optional] MAY contain a name that accurately identifies the Subscriber and includes the <i>ID</i> of the Quad ID.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

ICA Certificates issued under this CP SHALL assert the policy OID listed in Section 1.2.2 of this CP.

Table 37 shows the *certificatePolicies* extension settings for ICA Certificates and specifies that these Certificates:

- SHALL include the *certificatePolicies* extension; and
- SHALL set the criticality of the *certificatePolicies* extension to FALSE.

Table 37: *certificatePolicies* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
<i>certificatePolicies</i>		FALSE	{ id-ce 32 }	SHALL be included in ICA Certificates.
<i>policyIdentifier</i>	OID			See Section 1.2.2.

End-Entity Certificates issued under this CP SHALL assert the policy OID listed in Section 1.2.2 of this CP.

Table 38 shows the *certificatePolicies* extension settings for End-Entity Certificates and specifies that these Certificates:

- SHALL include the *certificatePolicies* extension; and
- SHALL set the criticality of the *certificatePolicies* extension to FALSE.

Table 38: *certificatePolicies* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
<i>certificatePolicies</i>		FALSE	{ id-ce 32 }	SHALL be included in End-Entity Certificates.
<i>policyIdentifier</i>	OID			See Section 1.2.2.

7.1.7 Usage of Policy Constraints Extension

None.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP SHALL NOT contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this CP SHALL NOT contain a critical *certificatePolicies* extension.

7.2 CRL Profile

CRLs issued by a CA under this CP SHALL conform to the CRL profile specified in [RFC 5280](#).

CRLs SHALL contain the basic fields and contents specified in the table below:

Table 39: CRL Profile Basic Fields

Field	Referenced Standard	Section	Requirement or Recommendation
<u><i>version</i></u>	[RFC 5280]	5.1.2.1	MUST specify version 2 (the integer value is 1).
<u><i>signature</i></u>	[RFC 5280]	5.1.2.2	This CP requires use of RSA signatures.
<u><i>issuer</i></u>	[RFC 5280]	5.1.2.3	This field details the entity that has signed and issued the CRL.
<u><i>thisUpdate</i></u>	[RFC 5280]	5.1.2.4	This field indicates the issue date of this CRL.
<u><i>nextUpdate</i></u>	[RFC 5280]	5.1.2.5	This field indicates the date by which the next CRL will be issued.
<u><i>revokedCertificates</i></u>	[RFC 5280]	5.1.2.6	When there are no Revoked Certificates, the <i>revokedCertificates</i> list MUST be absent. Otherwise, Revoked Certificates are listed by their serial numbers.
<u><i>authorityKeyIdentifier</i></u>	[RFC 5280]	5.2.1	
<u><i>cRLNumber</i></u>	[RFC 5280]	5.2.3	
<u><i>signatureAlgorithm</i></u>	[RFC 5280]	5.1.1.2	The <i>signatureAlgorithm</i> field contains the algorithm identifier for the algorithm used by the CRL issuer to sign the Certificate List. This field MUST contain the same algorithm identifier as the signature field in the sequence <i>tbsCertList</i> (RFC 5280, Section 5.1.2.2).
<u><i>signatureValue</i></u>	[RFC 5280]	5.1.1.3	

7.2.1 CRL Version Number(s)

The PCA and ICAs SHALL support the issuance of X.509 Version 2 CRLs. The CRL version number SHALL be set to the integer value of "1" for Version 2 [RFC 5280, Section 5.1.2.1].

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in [RFC 6960](#).

Critical CRL extensions SHALL NOT be used.

7.3 OCSF Profile

OCSF is a way to obtain timely information about the Revocation status of a particular Certificate. OCSF responses issued by a CA under this CP SHALL conform to the OCSF profile specified in [RFC 5280](#).

OCSF responses SHALL conform to [RFC 5019](#) and SHALL either be:

- Signed by the CA that issued the Certificates whose Revocation status is being checked; or
- Signed by an OCSF responder whose Certificate is signed by the CA that issued the Certificate whose Revocation status is being checked. Such OCSF responder Certificate SHALL contain the extension *id-pkix-ocsp-nocheck* as defined by [RFC 6960](#). This extension indicates that the End-Entity need not obtain a CRL for the OCSF responder's Certificate. The OCSF responder SHOULD be a highly trusted component.

7.3.1 OCSF Version Number(s)

CSSs operated under this CP SHALL use OCSF version 1 as defined by [RFC 6960](#) and [RFC 5019](#).

7.3.2 OCSF Extensions

Detailed CRL profiles addressing the use of each extension are specified in [RFC 6960](#).

8. Compliance Audit and Other Assessments

The PCA and ICAs, and the RAs on their behalf, SHALL have a Compliance Audit mechanism in place to ensure that the requirements of this CP are being implemented and enforced. CAs SHOULD have self-Auditing capability and SHOULD complete self-Audits quarterly.

This CP does not impose a requirement for any particular assessment methodology other than that noted below.

8.1 Frequency or Circumstances of Assessment

CAs and RAs SHALL be subject to a periodic Compliance Audit at least once per year. In addition, the appropriate PA MAY require an Audit should circumstances dictate.

8.2 Identity and Qualifications of Assessor

The Compliance Auditor MUST demonstrate competence in the field of Compliance Audits, and MUST be thoroughly familiar with CAs, RAs, and CPs. The Compliance Auditor MUST perform such Compliance Audits as a regular ongoing business activity. In addition to the previous requirements, the Compliance Auditor MUST be a Certified Information Systems Auditor or IT security specialist, and a PKI Subject matter specialist who can offer input regarding acceptable Risks, mitigation strategies, and industry best practices. The CA and RA MAY identify the parties responsible for providing such services, and the mechanisms used to support these services.

8.3 Assessor's Relationship to Assessed Entity

The Compliance Auditor either SHALL be a private firm that is independent from the entities (CA or RA) being Audited, or it SHALL be sufficiently and organizationally separated from those entities to provide an unbiased, independent evaluation. To ensure independence and objectivity, the Compliance Auditor MUST NOT have served the entity in developing or maintaining the to-be-Audited CA Facility. The appropriate PA SHALL determine whether a Compliance Auditor meets this requirement.

8.4 Topics Covered by Assessment

The Audit MUST conform to industry standards (e.g., WebTrust for CA Audits), cover the CA's and RA's compliance with this CP and the relevant CPS, and evaluate the Integrity of the CA's PKI operations and RA's operations. The Audit MUST verify that each CA and RA is compliant with this CP.

8.5 Actions Taken as a Result of Deficiency

When the Compliance Auditor finds a discrepancy between the requirements of this CP and the design, operation, or maintenance of the PKI, the following actions SHALL be performed:

- The Compliance Auditor SHALL note the discrepancy;
- The Compliance Auditor SHALL notify the responsible party promptly of the discrepancy;

- The party responsible for correcting the discrepancy SHALL determine what further notifications or actions are necessary pursuant to the requirements of the applicable CPS, create a written plan with committed dates and then proceed to make such notifications and take such actions without delay. This plan, with dates, SHALL be given to the appropriate PA, which MUST approve it;
- The responsible party SHALL provide the appropriate PA with regular progress reports and notify the appropriate PA when corrective actions have been completed; and
- The Compliance Auditor SHALL be notified when corrective actions have been completed and MAY repeat portions or the entirety of the Audit to confirm the discrepancy has been addressed to the satisfaction of the Compliance Auditor.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the appropriate PA MAY decide to temporarily halt operation of its corresponding CA, to Revoke a Certificate issued by the CA or its corresponding RA, or take other actions it deems appropriate. The appropriate PA SHALL provide to the CA its procedures for making and implementing such determinations.

8.6 Communication of Results

The CA MUST submit an annual Compliance Audit report to the PCA PA, with an assertion from the Auditor that all PKI components have been Audited - including any components that are separately managed and operated.

8.7 Internal Audits

The PCA and ICAs SHALL perform regular internal Audits of its operations, personnel, and compliance with this CP. Results of these Audits SHALL be made available to the Compliance Auditor.

9. Other Business and Legal Matters

9.1 Fees

Any fees SHALL be approved by the PA and (if applicable) the ICA PA, if the ICA PA institutes fees in addition to those instituted by the PA.

Fees for services defined in this CP are agreed to by the PA and PCA in their Master Service Agreement (MSA). Any changes to the services required in the CP (e.g., cross-certification with another CA) will be evaluated by the PCA upon request from the PA. The scope and cost to implement the change will be negotiated in good faith and the MSA will be amended accordingly.

9.1.1 Certificate Issuance or Renewal Fees

Subscribers MAY be charged a fee for the issuance, management, and Renewal of Certificates. These fees will be proposed by the MA, agreed to by the appropriate PA, and will be available to Prospective Subscribers.

9.1.2 Certificate Access Fees

Section 2.4 of this CP requires that CA Certificates and CRLs be publicly available. The PCA and ICAs operating under this CP MUST NOT charge additional fees for Access to this information.

9.1.3 Revocation or Status Information Access Fees

CAs operating under this CP MUST NOT charge additional fees for Access to Certificate status information.

9.1.4 Fees for other Services

No stipulation.

9.1.5 Refund Policy

To be proposed by the MA and agreed to by the appropriate PA.

9.2 Financial Responsibility

This CP contains no limits on the use of Certificates issued by CAs under the policy. The CA, RA, PA, ICA PA and MA assume no liability for any use of the Certificates.

9.2.1 Insurance Coverage

To be addressed in the MSA between the PA and the PCA for the PCA. For ICAs, to be addressed in the agreement between the MA and the ICA.

9.2.2 Other Assets

Not Applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

The PCA and ICAs, and the RAs on their behalf, SHALL protect the Confidentiality of sensitive information stored or processed on CA systems that could lead to abuse or fraud. RAs SHALL protect customer data that could allow an attacker to impersonate a customer.

Public Access to organizational information SHALL be determined by the respective organization.

9.3.1 Scope of Confidential Information

Confidential information means all information in written or oral form that the disclosing party identifies as confidential, and any trade secret or other proprietary information that the recipient knows or reasonably should know is intended to be treated as confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Information that is generally known to the public or properly known by the receiving party at the time of disclosure and other typical exceptions is not within the scope of confidential information.

9.3.3 Responsibility to Protect Confidential Information

Any party that collects, transmits, or stores confidential information SHALL be responsible for ensuring it SHALL NOT be released except as required by law.

9.4 Privacy of Personal Information

It is the responsibility of all parties to ensure Privacy of personal information under their control. No personal information is registered or certified. Information about ICA operators is retained by the PCA as part of the certification request, which is subsequently logged and later Archived. If a party collects, transmits, or stores personal information, its practices will comply with all applicable laws.

9.4.1 Privacy Plan

The PCA and ICAs, and the RAs on their behalf, SHALL each develop, implement, and maintain a Privacy plan. The Privacy plan SHALL document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information MAY be disclosed.

9.4.2 Information Treated as Private

CAs and RAs SHALL protect all Subscriber personally identifiable information from unauthorized disclosure. Records of individual transactions MAY be released upon request of any Subscribers involved in the transaction or their legally recognized Agents. The contents of the Archives maintained by CAs operating under this CP SHALL NOT be released, except as required by the Privacy plan.

9.4.3 Information Not Deemed Private

Information included in Certificates is not subject to protections outlined in Section 9.4.1, but MAY NOT be sold to a third party.

9.4.4 Responsibility to Protect Private Information

Sensitive information MUST be stored securely, and MAY be released only in accordance with other stipulations in Section 9.4.

9.4.5 Notice and Consent to Use Private Information

CAs or RAs are not required provide any notice or obtain the consent of the Subscriber in order to release private information in accordance with other stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

CAs or RAs SHALL NOT disclose private information to any third party unless authorized by this CP, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

No party will use any property owned by any other party, including, without limitation, any trademark, copyright, trade secret or other proprietary right, unless they have been licensed that use

PKI Participants SHALL NOT knowingly violate Intellectual Property Rights held by others and SHALL NOT knowingly claim to represent an Agency or role that the party does not credibly represent. Without limitation, except as the intellectual property owner or a Trusted Person credibly representing an Agency MAY expressly authorize in writing, it is prohibited to:

- Reverse engineer, translate, disassemble, decompile the whole or any part of any software or system or any part thereof, or otherwise attempt to Access any software source code embedded in or used in the operation of any system;
- Assign, transfer, sell, license, sub-license, lease, rent, charge or otherwise deal in or encumber, any software or system or any part thereof, or use same on behalf of or for the benefit of any third party, or make available the same in any way whatsoever to any third party without prior written consent;
- Remove or alter any trademark or any copyright or other proprietary notice on any software, system or any other materials;
- Distribute, create derivative works of or modify any materials, software or systems or any part thereof in anyway, or use, copy, duplicate or display same on a commercial or development basis; and

- Provide any service using a Certificate provided under this CP except as authorized and provided in this CP and an approved CPS.

These restrictions SHALL NOT be construed in a manner that would violate any applicable law.

The PA SHALL be deemed the owner of the keys for all Hosted ICAs.

9.6 Representations and Warranties

The PA SHALL:

- Approve the CPS for CAs issued by the PCA under this CP.

The obligations described below pertain to the MA, on behalf of the PA.

The MA SHALL:

- Review name space control procedures to ensure that DNS are uniquely assigned for all Certificates issued under this CP;
- Distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

9.6.1 CA Representations and Warranties

CAs operating under this CP SHALL comply with the stipulations of this CP, and comply with a CPS approved by the PA for use with this CP. The CA warrants that any Certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this CP.

A CA that issues Certificates that assert a policy defined in this CP SHALL conform to the stipulations of this CP, including:

- Providing a CPS to the appropriate PA, as well as any subsequent changes, for conformance assessment;
- Maintaining its operations in conformance to the stipulations of the CPS;
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS;
- Including only valid and appropriate information in Certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the Certificates;
- Revoking the Certificates of Subscribers found to have acted in a manner counter to their obligations in accordance with Section 9.6.3; and
- Operating or providing for the services of an online Repository, and informing the Repository service provider of their obligations if applicable.

9.6.2 RA Representations and Warranties

A RA that performs registration functions as described in this CP SHALL comply with the stipulations of this CP, and comply with a CPS approved by the appropriate PA for use with this CP. A RA who is found to have acted in a manner inconsistent with these

obligations is subject to Revocation of RA responsibilities. A RA supporting this CP SHALL conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of the approved CPS;
- Including only valid and appropriate information in Certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the Certificate; and
- Ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

To the extent permitted by applicable law, the RA disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose.

9.6.3 Subscriber Representations and Warranties

A Subscriber SHALL sign a DCSA to acknowledge acceptance of the requirements the Subscriber SHALL meet, including protection of their Private Keys and use of the Certificates before being issued the Certificate.

In addition, Subscribers SHALL:

- Accurately represent themselves in all communications with the PKI authorities;
- Protect their Private Key(s) at all times, in accordance with this CP, and as stipulated in their DCSA;
- Promptly notify the appropriate CA upon suspicion of loss or Compromise of their Private Key(s). Such notification SHALL be made directly or indirectly through mechanisms consistent with the CA's CPS; and
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Key(s) and Certificate(s).

DCSAs MAY include additional representations and warranties.

9.6.4 Relying Parties Representations and Warranties

This CP does not specify the steps a Relying Party SHOULD take to determine whether to rely upon a Certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., Certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the Relying Party MAY wish to employ in its determination.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

PAs, MAs, CAs, RAs, and Subscribers operating under this CP SHALL NOT disclaim any of their responsibilities described in this CP.

9.8 Limitations of Liability

The PCA SHALL NOT be liable for any indirect damages of any kind, including consequential, incidental, special, punitive, or other damages whatsoever arising out of or related to this CPS, even if advised of the possibility of such damages.

The liability (and/or limitations thereof) of Subscribers SHALL be as set forth in the applicable DCSAs.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP SHALL be effective from the PA approval date, and SHALL remain effective until replaced. Amendments to this CP become effective upon publication.

9.10.2 Termination

Termination of this CP is at the discretion of the PA.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the Archive period for the last Certificate issued.

9.11 Individual Notices and Communications with PKI Participants

The PA SHALL establish appropriate procedures for communications with CAs operating under this CP via contracts or memoranda of agreements as applicable.

For all other communications, no stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The PA SHALL review this CP at least once every year. Corrections, updates, or changes to this CP SHALL be made publicly available. Suggested changes to this CP SHALL be communicated to the contact in Section 1.5.2; such communication MUST include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification Mechanism and Period

Whenever the CP is amended, the PA SHALL published it within five (5) days of the date the amendment took place and all known concerned parties (CA staff, Relying Parties, Subscribers, etc.) SHALL be notified.

9.12.3 Circumstances Under Which OID Must be Changed

CP OIDs SHALL be changed if the CA determines that a change in this CP decreases the level of assurance provided.

9.13 Dispute Resolution Provisions

The PA SHALL facilitate the resolution between entities when conflicts arise as a result of the use of Certificates issued under this CP.

9.14 Governing Law

The construction, validity, performance and effect of Certificates issued under this CP for all purposes SHALL be governed by United States Federal, state or local law, or applicable national law (statute, case law, or regulation), as appropriate.

9.15 Compliance with Applicable Law

All CAs operating under this CP SHALL comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by contract, no party MAY assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party (such consent not to be unreasonably withheld), except that the PA MAY assign and delegate this CP to any party of its choosing.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP SHALL remain in effect until this CP is updated. The process for updating this CP is described in Section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Any failure to exercise any right hereunder SHALL NOT be construed as a relinquishment of any future exercise of such right.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

Appendices

Appendix A - Abbreviations and Acronyms

This document uses the following abbreviations and acronyms:

AIA	Authority Information Access
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSS	Certificate Status Service
DCSA	Digital Certificate Subscriber Agreement
DN	Distinguished Name
DRP	Disaster Recovery Plan
ESInet	Emergency Services IP Network
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
MA	Management Authority
MOA	Memorandum of Agreement
MSA	Master Service Agreement
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NIOC	NG9-1-1 Interoperability Oversight Commission
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

PCA	PSAP Credentialing Agency
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PSAP	Public Safety Answering Point
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SAN	Subject Alternative Name
SHA	Secure Hash Algorithm
SP	Special Publication
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VP	Validation Policy

Appendix B - Glossary

This document uses the following terms and definitions:

Term	Definition
Access	Ability to make use of any Information System resource. [CNSSI 4009]
Access Control	Process of granting Access to Information System resources only to authorized users, programs, processes, or other systems. [CNSSI 4009]
Account Administrator	An employee or other Trusted Person authorized to perform PKI tasks via the RA on behalf of the Subscriber.
Activation Data	Private data, other than keys, that are required to Access Cryptographic Modules (i.e., unlock Private Keys for signing or decryption events).
Agency	Defined in CP Section 1.3.7.2.
Agency Certificate	An End-Entity Certificate issued to an Agency. ID example: psap.fairfax.virginia.us.
Agency Representative	Defined in CP Section 1.3.7.2.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Term	Definition
Agent Certificate	An End-Entity Certificate issued to a person. ID example: dhandy@psap.fairfax.virginia.us.
Anonymous	Having an unknown or undisclosed name.
Applicant	See "Prospective Subscriber."
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of Records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [CNSSI 4009]
Audit Data	Chronological Record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [CNSSI 4009, "Audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [CNSSI 4009]
Authentication Certificate	An End-Entity Certificate used for Authentication in which the Subject is not a CA. Element, Agent and Agency Certificates are all Authentication Certificates.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two (2) related elements of information. [CNSSI 4009]
Biometric	A physical or behavioral characteristic of a human being.
CA Administrator	An employee or other Trusted Person authorized to perform PKI tasks on behalf of the CA.
CA Facility	The collection of equipment, personnel, procedures, and structures that are used by a CA to perform Certificate issuance and Revocation.
CA Operations Staff	CA components are operated and managed by individuals holding trusted, sensitive roles.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Term	Definition
Certificate	A digital representation of information which at least: • Identifies its issuing CA • Names or identifies the Subscriber of the Certificate • Contains the Subscriber's Public Key • Identifies its operational period • Is digitally signed by the issuing CA As used in this CP, the term "Certificate" refers to X.509 Certificates that expressly reference the OID of this CP in the <i>certificatePolicies</i> extension.
Certificate Application	A request from a Prospective Subscriber that is also called the Naming Application (which is part of the DCSA), containing the naming information that will be included in the End-Entity Certificates (customer profile information and Naming Application that will set the Subject DN in the Certificates).
Certificate Policy (CP)	A CP is a specialized form of administrative policy that conforms to RFC 3647 and consists of a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.
Certificate Revocation List (CRL)	A list maintained by a CA of the Certificates that is has issued that are Revoked prior to their stated expiration date.
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certificate Status Service (CSS)	A trusted entity that provides online verification to a Relying Party of a Subject Certificate's Revocation status, and MAY also provide additional attribute information for the Subject Certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
Certification Practice Statement (CPS)	A statement of the practices which a CA employs in issuing Certificates.
Compliance Audit	A periodic Audit that a CA system undergoes to determine its conformance with PKI requirements that apply to it.
Compliance Auditor	An individual (e.g., employee, contractor, consultant, third party) who is responsible for Auditing the security of CAs or RAs, including reviewing, maintaining, and archiving Audit logs; and performing or overseeing internal Audits of CAs or RAs. A single individual MAY Audit both CAs and RAs. Compliance Auditor is an external role that is designated as trusted.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Term	Definition
Compromise	Disclosure of information to unauthorized persons, or a violation of the Security Policy of a system in which unauthorized intentional or unintentional disclosure, Modification, destruction, or loss of an object may have occurred. [CNSSI 4009]
Confidentiality	Preserving authorized restrictions on information Access and disclosure, including means for protecting personal privacy and proprietary information.
Cross-Certificate	A Certificate used to establish a trust relationship between two (2) CAs.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140-2]
Digital Certificate Subscriber Agreement (DCSA)	An agreement setting forth the terms and conditions under which an organization acts as a Subscriber. The DCSA contains the Certificate Application.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine (1) whether the transformation was created using the Private Key that corresponds to the Public Key in the signer's digital Certificate; and (2) whether the message has been altered since the transformation was made.
Disaster Recovery Plan (DRP)	A documented process or set of procedures to recover and protect an infrastructure in the event of a disaster.
Discrete ICA	An ICA operated by the Subscriber or a third-party PKI service provider on behalf of the Subscriber.
Distinguished Name (DN)	Identification fields in a Certificate that are input by the CA when issuing Certificates. The information is obtained from the Subscriber's Certificate Application.
Element Certificate	A Certificate issued to a physical or virtual entity that is addressable and has a unique identity (<i>elementId</i>).
End-Entity Certificate	A Certificate issued to a Subscriber (also known as a Subscriber Certificate) used for either Authentication or signing.
Firewall	Gateway that limits Access between networks in accordance with local Security Policy. [CNSSI 4009]
Hardware Security Module (HSM)	A physical computing device that safeguards and manages digital keys for strong Authentication and provides crypto processing.
Hosted ICA	An ICA that is hosted by DigiCert in its PKI facilities.
Information System	An integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Term	Definition
Integrity	Protection against unauthorized modification or destruction of information. [CNSSI 4009] A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property Rights	Rights under one or more of the following: copyright, patent, trade secret, trademark, trade name, or any other Intellectual Property Rights.
Intermediate CA (ICA)	A CA subordinate to the PCA or another ICA and operates according to this CP.
Key Generation Ceremony	A procedure whereby a CA's Key Pair is generated, its Private Key is backed up, and/or its Public Key is certified.
Key Pair	Two (2) mathematically related keys having the properties that (1) one (Public) Key can be used to encrypt a message that can only be decrypted using the other (Private) Key; and (2) even knowing the Public Key, it is computationally infeasible to discover the Private Key.
Key Rollover Certificate	The Certificate that is created when a CA signs a new Public Key for itself with its old Private Key, and vice versa.
Management Authority (MA)	An entity whose role is to provide management services to support the ecosystem in meeting its security goals.
Modification (of a Certificate)	The act or process by which data items bound in an existing Public Key Certificate, especially authorizations granted to the Subject, are changed by issuing a new Certificate.
Naming Application	A form, included in the Certificate Application, that is completed by the Prospective Subscriber and contains the information to be loaded into the Certificate Subject DN which will set the Certificate profile.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In this PKI, OIDs are used to uniquely identify Certificate Policies and cryptographic algorithms.
Online Certificate Status Protocol (OCSP)	An Internet protocol used for obtaining the Revocation status of a X.509 digital Certificate.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a CSR.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Term	Definition
PKI Participant	An individual or organization that is one or more of the following within the PKI: a CA, a Subscriber, or a Relying Party.
PKI Sponsor	When the Subscriber is a device, an authorized representative of the device will act as the PKI Sponsor.
Policy Authority (PA)	Body established to oversee the creation and update of Certificate Policies, review CPSs, review the results of CA Audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI Certificate Policies.
Privacy	Restricting Access to Subscriber or Relying Party information in accordance with Federal law.
Private Key	The key of a signature Key Pair used to create a Digital Signature. This key MUST be kept secret.
Prospective Subscriber	The Subscriber, sometimes called an "Applicant", is known as a Prospective Subscriber while going through the Certificate issuance process, until the point when the Certificate issuance procedure is completed (e.g., when the Certificate has been issued).
Pseudonym	A Subscriber name that has been chosen by the Subscriber that is not verified as meaningful by identity proofing. [CNSSI 4009]
Public Key	The key of a signature Key Pair used to validate a Digital Signature. This key is normally made publicly available in the form of a digital Certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, service platforms, software and workstations used for the purpose of administering Certificates and Public-Private Key Pairs, including the ability to issue, maintain, and Revoke Public Key Certificates.
Records	A thing constituting a piece of evidence about the past, especially an account of an act or occurrence kept in writing or some other permanent form.
Registration Authority (RA)	An entity in a PKI (separate from the CA) that is responsible for identification and Authentication of Certificate Subjects, but that does not sign or issue Certificates (i.e., a RA is delegated certain tasks on behalf of an authorized CA). The RA MAY also perform other Certificate management functions for the CA.
Re-Key (a Certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new Certificate that contains the new Public Key.
Relying Party	A person or entity that receives a Certificate with a Digital Signature verifiable with the Public Key listed in the Certificate, and is in a position to assess the trust in the Authentication information provided by the Certificate depending on the CP governing the PKI and the Certificate verification.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Term	Definition
Renew (a Certificate)	The act or process of extending the validity of the data Binding asserted by a Public Key Certificate by issuing a new Certificate.
Repository	A database containing information and data relating to Certificates as specified in this CP; MAY also be referred to as a directory.
Revocation	The process of canceling (or revoking) a Certificate.
Revoke (a Certificate)	To prematurely end the operational period of a Certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular Threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose Public Key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. A Root CA is the highest-level CA of a PKI. It generates a self-signed Certificate, which means that the Root CA validates itself (self-validating). A Root CA can issue ICAs that effectively trust it. The ICAs receive a Certificate signed by the Root CA, so the ICAs can issue Certificates that are validated by the Root CA. This establishes a CA hierarchy and chain of trust.
Security Auditor	An individual (e.g., employee, contractor, consultant, third party) who is responsible for Auditing the security of CAs or RAs, including reviewing, maintaining, and archiving Audit logs; and performing or overseeing internal Audits of CAs or RAs. A single individual MAY Audit both CAs and RAs. Security Auditor is an internal role that is designated as trusted.
Security Policy	The highest-level document describing an organization's Security Policies.
Signing Certificate	An End-Entity Certificate used for Signing in which the Subject is not a CA..
Subject	The holder of a Private Key corresponding to a Public Key. The term "Subject" can refer to the Subscriber who is issued the Certificate.
Subscriber	A Subscriber is an entity that (1) is the Subject named or identified in a Certificate issued to that entity, (2) holds a Private Key that corresponds to the Public Key listed in the Certificate, and (3) does not itself issue Certificates to another party. This includes, but is not limited to, an individual, an application, or a network device.
Threat	Any circumstance or event with the potential to cause harm to an Information System in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [CNSSI 4009]
Trust Anchor	The Root Certificate from which the chain of trust for a PKI is derived.

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Term	Definition
Trusted Person	An employee, contractor, or consultant of an entity within a PKI, responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
Trusted Role	Those roles Identified in Section 5.2.1.
Validity Period	The period starting with the date and time a Certificate is issued and ending with the date and time on which the Certificate expires or is Revoked.

Appendix C - References

This document uses the following references:

Doc Number	Reference Title
CNSSI 4009	CNSSI 4009, Committee on National Security Systems Glossary, April 6, 2015 https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
CVSS	Common Vulnerability Scoring System v3.1: Specification Document. https://www.first.org/cvss/v3.1/specification-document
FIPS 140-2	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001; (Change Notice 2, 12/3/2002), is available at: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
FIPS 186-4	Digital Signature Standards (DSS), FIPS 186-5, February 2023. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FPKIPA	X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework, version 2.5, July 6, 2023. https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf
NENA i3	NENA i3 Standard for Next Generation 9-1-1, STA-010.3-202x, https://www.nena.org/page/standards#CoreServices
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels (Bradner), March 1997 https://www.ietf.org/rfc/rfc2119.txt
RFC 2560	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999. http://www.ietf.org/rfc/rfc2560.txt
RFC 3647	Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003. https://www.ietf.org/rfc/rfc3647.txt
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, IETF (Deacon, and Hurst), September 2007. https://www.ietf.org/rfc/rfc5019.txt

Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy

Doc Number	Reference Title
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 https://www.ietf.org/rfc/rfc5280.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013 https://www.ietf.org/rfc/rfc6960.txt
SP 800-63	NIST Special Publication 800-63, Digital Identity Guidelines document suite, https://pages.nist.gov/800-63-3/
SP 800-88-1	NIST Special Publication 800-88, Rev 1: Guidelines for Media Sanitization https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
VP	NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines, February 2022. https://ng911ioc.org/wp-content/uploads/2022/02/NIOC-PCA-Validation-Policy-v1.0-02-09-2022-CLEAN.pdf
X.500	ITU-T Recommendation X.500 Series (1994) – ISO/IEC 9594,1-9:1994, <i>Information Technology – Open Systems Interconnection – The Directory</i>

Exhibit 9 Service Level Agreement

Motorola Call Routing Service: Standard Service Levels

Version 1.3 January 8, 2025

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this budgetary estimate. Motorola Solutions Connectivity Confidential Restricted

Table of Contents

Table of Contents 2

Section 1..... 3

Severity Level: Response and Communication Times 3

Section 2..... 4

Definitions..... 4

Response Time..... 4

Valid Destination 4

Service Demarcation..... 4

Incident Time 4

Critical Severity 4

High Severity 4

Medium Severity 4

Low Severity 4

Section 3..... 5

Service Credits 5

3.1 Performance Service Credits - Motorola Call Routing Service 5

3.2 Monthly Remedy Entitlement 6

3.3 Exclusions to Service Credits..... 7

3.4 Incident Status and Event Analysis Report 8

3.5 Service Event Mitigation 8

Section 1

Severity Level: Response and Communication Times

For each reported service request or alert generated Critical, High, Medium, or Low incident (as defined below), the Motorola Solutions Connectivity, Inc. (Motorola) Network Security Operations Center (NSOC) will apply a severity level classification with an assigned target response time where applicable. This classification provides the means to manage the appropriate response and engagement process.

Severity	Target Response Time	Description	Anticipated Communication Interval
Critical (P1) 24 x 7 x 365	Within 15 minutes, a notification will be provided.	Significant and/or severe degradation of service functionality that impacts inbound call or associated location processing, with no workaround available.	Hourly
High (P2) 24 x 7 x 365	Within 30 minutes, notification will be provided.	Significant degradation of service functionality that impacts inbound call or associated location processing where a workaround may be available.	Every 2 hours
Medium (P3) 24 x 7 x 365	Within 4 hours, notification will be provided.	A minor degradation of service functionality or capacity of inbound call or associated location processing.	Daily
Low (P4) 8/5/ Next Business Day (Excluding Holidays)	Next business day.	A degradation of system functionality that does not impact inbound call or associated location processing.	Updates as needed via Email &/or Motorola Customer Hub

Section 2

Definitions

Response Time

Response Time shall be defined as the duration of time expired between the time in which the issue is either (a) detected by the NSOC or (b) reported to the NSOC by the Customer to the time that a qualified technician is actively troubleshooting the issue. The NSOC Service Management system timestamps shall be used to measure response time.

Valid Destination

A valid destination means the correct primary or alternative PSAP, Public Switch Telephone Network (PSTN) or tone/treatment.

Service Demarcation

The inbound Service Demarcation point is the Point of Interface (POI) that connects to the Originating Service Provider (OSP).

Incident Time

Incident Time means the period of time during which the service or any service component suffers an incident. Incident Time shall commence upon either the issue is (a) detected by the Motorola NSOC or (b) reported to the NSOC by the Customer. Incident Time shall end upon completion of the repair or restoration of the service or service component. Incident Time shall not include downtime attributable to (a) Force Majeure conditions; or (b) scheduled preventive maintenance of which the Customer was notified.

Critical Severity

An incident shall be categorized as a “Critical Severity” if the incident is characterized whereby the Service or its critical components are completely inoperative or non-functional.

High Severity

An incident shall be categorized as a “High Severity” if the incident is characterized whereby the Service is degraded and functioning at a limited capacity or critical functions are no longer redundant.

Medium Severity

An incident shall be categorized as a “Medium Severity” if the incident is defined as a reported problem disabling specific non-essential functions or resulting in Customer inconvenience; error condition is not critical to continuing operation and/or Motorola has determined a work around for the error condition.

Low Severity

An incident shall be categorized as a “Low Severity” if the incident is characterized where the services are impaired and some functions are not operating, but the impairments are considered minor or cosmetic and have only a minor impact on usability. An informational request or questions of a general nature concerning the overall product suite functionality.

Section 3

Service Credits

Motorola has included a robust Service Credit program that offers remedies should our NG9-1-1 service fall below the agreed Service Levels.

As a remedy to compensate Customers with service level credits where Motorola fails to meet relevant SLAs and for reliability review and tracking purposes, the Customer must (a) open a trouble ticket within 2 weeks of the occurrence of the issue and (b) notify Motorola in writing of a claim within six (6) months of the day Motorola failed to meet the service level. All claims submitted by Customer shall include the date and time of the incident that Customer believes makes it eligible for an SLA service credit.

Any SLA credit paid to Customer shall constitute the Customer's sole and exclusive remedy for Motorola failure to meet an SLA.

3.1 Performance Service Credits - Motorola Call Routing Service

Performance Measure	Motorola Call Routing Service, Call Delivery
Description	The Call Delivery performance objective for the PSAPs includes all calls received into the Motorola Call Routing Service in any specified calendar month are delivered to a Valid Destination (i.e. the call handling system hosts.) This does not include: (1) calls in the setup stage of call processing and which are abandoned (by the caller) before the call setup processing has completed, or (2) calls for which the Call Handling System and/or PSAP is unavailable. If the Call Delivery performance objective is not met in a specified month (the "Failure Month") and Motorola fails to remedy the issues within one (1) month following the Failure Month, the Customer will receive a credit.
Measure	The objectives of the service level include (i) if less than 100,000 calls are presented to Motorola Call Routing Service in a specified month, and a Valid Destination receives at least one (1) call of the total calls presented to Motorola Call Routing Service for that Valid Destination; or (ii) if 100,000 or more calls are presented to Motorola Call Routing Service in a month, and a Valid Destination PSAP receives at least 0.001% of the total calls presented to Motorola Call Routing Service for that Valid Destination.
Remedy	A credit of 5% for the monthly recurring charge for the Motorola Call Routing Service for the PSAP(s) that is/are impacted will be provided if the service performance objective is not met in a specified calendar month.

Performance Measure	Voice
Description	Motorola will monitor the IP audio packets from the Motorola Call Routing Service egress demarcation point into the ESInet to the demarcation point associated with the PSAP call handling system/service.
Measure	The objective is for the daily Predicted Mean Opinion Score (PMOS) value per PSAP to not be less than a 3.5 threshold for G.711 codec as measured by Motorola, where the ideal PMOS score for the G.711 codec is 4.3 as measured by Motorola. The daily PSAP PMOS value will be based on an average of the per call PMOS scores over a 24 hour calendar day. If the Voice Quality falls below the target for three consecutive days in a calendar month and Motorola is unable to restore Motorola Call Routing Service to the SLA target within 30 days, the Customer will receive a credit.
Remedy	A credit of 5% for the monthly recurring charge for the Motorola Call Routing Service for the PSAP(s) that is/are impacted will be provided if the service performance objective is not met in a given calendar month.

Performance Measure	Motorola Call Routing Service, Service Availability
Description	Service Availability of the Motorola Call Routing Service will be supported which measures the availability requirement of 99.999% for Call Routing. Call Routing is the ability of the Service to accept new 911 requests for service and deliver calls from the inbound Service Demarcation point from the Origination Service Provider (OSP) to a Valid Destination. Downtime for the Service Availability will not exceed 5.26 minutes per year.
Measure	The Service Availability is calculated from the time an issue is reported that impacts Call Routing Service availability, until such time that the Call Routing Service availability is restored. If the Service Availability falls below the target of 99.999% within a calendar year, the Customer will receive a credit.
Remedy	A credit of 50% of a monthly recurring charge for the Motorola Call Routing Service for the PSAP(s) that is/are impacted will be provided if the service performance objective is not met within a given calendar year.

3.2 Monthly Remedy Entitlement

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this budgetary estimate. Motorola Solutions Connectivity Confidential Restricted

Customers may not receive SLA credits totaling more than 50% of the monthly charge for any affected PSAP for a given calendar month.

3.3 Exclusions to Service Credits

The following exclusions apply to all Service Credits:

1. No Service Credits will be due where routing failures are related to GIS database inaccuracies in data received from the Customer.
2. No Service Credit will be due to the extent the Incident Time is not met because the incident is the result of an act or omission on the part of the Customer, or its contractors.
3. If the Incident Time is not met because Motorola is delayed in or prevented from responding to or restoring a service component or equipment because of any act or omission on the part of the Customer, then the time used to measure the Incident Time will be correspondingly stated to reflect the amount of time that Motorola was delayed in or prevented from responding or restoring such service component or equipment.
4. No Service Credit will be due to the extent the Incident Time is not met because of a Force Majeure event (as defined in the applicable Master Service Agreement) directly impacting the Customer or Motorola infrastructure.
5. No Service Credit will be due during periods of scheduled work by Motorola including maintenance and new installations of hardware and/or software that have been approved through the Change Management Request Process or Customer approval. Notwithstanding the foregoing, Motorola will take commercially reasonable efforts to prevent scheduled maintenance and new installations from impacting support and the Incident Time. However, should an incident occur during periods of scheduled work by Motorola that persists beyond completion of the scheduled work or should an incident occur which is caused by service components not reasonably related to the scheduled work, a Service Credit will apply where applicable.
6. No Service Credit will be due if the incident is resulting from network devices or malware (e.g., viruses, worms, etc.) unless Motorola is determined to be solely responsible for introducing such unapproved device or malware.
7. No Service Credits will be due if the parties agree that the incident results in a "No Trouble Found" trouble ticket.
8. No Service Credits will be due if the Incident Time is not met because of the Customer's material non-compliance with any obligation under the Agreement to the extent such noncompliance is a substantial contributing factor to Motorola's failure to meet the Incident Time.
9. No Service Credits will be due resulting from a PSAP/Host location that has not been actively in- use (calls made to or from the PSAP/Host location) for a minimum of 30 calendar days (Call Delivery, Voice Quality, Service Availability)
10. No Service Credits will be due to service interruptions, deficiencies, degradations or delays;
 - A. associated with ESInet network connections or local access beyond the call handling system/service demarcation point;
 - B. due to actions taken by Customer resulting in call quality issues (For example: CPE trunk volume power too high/low, Customer equipment);
 - C. due to lack of capability or by faulty call handling equipment and software; Customer not ordering sufficient bandwidth/concurrent call capacity;
 - D. test calls or call with a duration of less than 10 (ten) seconds;
 - E. days where a PSAP receives less than 20 calls per day for the purpose of

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this budgetary estimate. Motorola Solutions Connectivity Confidential Restricted

the Voice Quality SLA.

11. If a Customer is entitled to more than one Service Credits for the same service interruption, deficiency, degradation or delay; then only one Service Credit shall apply.

3.4 Incident Status and Event Analysis Report

Motorola operates a Service Management system (ServiceNow) for tracking and reporting troubles (incidents). Via the Customer Web Portal (CWP), there is a service page for opening trouble tickets, submitting change requests, and checking status of existing items.

Motorola prepares and submit a preliminary event analysis report (EAR) within 3 business days for Critical events. The preliminary report will provide an overview of all information known at that time. A final report will also be provided that describes the cause, resolution and any preventative steps that can be taken to eliminate future events.

3.5 Service Event Mitigation

In the event of a critical service impacting event, Motorola applies immediate and sustained efforts until Services are restored. Motorola uses all reasonable efforts to provide a temporary workaround within an agreed upon time frame of the issue being detected. If a temporary workaround solution is provided, Motorola will provide an action plan to be mutually agreed upon for the final resolution. We continue resolution activity until full service is restored. The primary objective of an incident is to mitigate impact. The Incident Manager is able to call upon whatever resources are required to identify and restore functionality on a 7x24 basis.

Exhibit 10 Sample Support Plan



MOTOROLA SOLUTIONS

Next Generation Core Services Sample Support Plan

Motorola Solutions Connectivity, Inc., is a wholly owned subsidiary of Motorola Solutions, Inc. This document is protected by copyright law and international treaties, and is the information of Motorola Solutions Connectivity, Inc. All trademarks, service marks, product names, brands, company names and logos appearing in this document are the property of their respective owners. VESTA® is a registered trademark of Motorola Solutions Connectivity, Inc.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2026 All rights reserved.

Table of Contents

Section 1

Quick Contacts 2

 1.1 Escalation Contact Information..... 3

Section 2

Support Plan Summary 4

 2.1 Introduction 4

 2.2 Service Management Overview 4

Section 3

Service Delivery and Support.....6

 3.1 Customer Service Manager..... 6

 3.2 Motorola Network Security Operations Center..... 6

 3.3 Reporting Incidents 6

 3.4 Priority Level and Response Definitions 7

 3.5 Customer Hub..... 9

 3.6 Support Engineer 9

 3.7 Service Maintenance 9

 3.8 Maintenance Process 9

Section 4

FCC and State Reporting 10

 4.1 Customer Notification 10

Section 5

Requesting a Service Change 12

 5.1 Requesting a GIS Change Impacting Call Routing..... 12

Section 6

Conditions and Exclusions.....13

 6.1 Conditions..... 13

 6.2 Exclusions 13

Section 1

Quick Contacts

Table 1 Quick Contacts

QUICK CONTACTS	
Motorola Support Center	
Phone	800.MSI.HELP (674.4357)
Email	VestaNSOC@MotorolaSolutions.com
Customer Hub Website	https://customerhub.motorolasolutions.com
Customer Hub Support Email	portal.support@motorolasolutions.com
Provide the following information:	1. Site Name 2. Site ID Number 3. Your Name 4. Your Callback Number 5. A Brief Description of the Problem 6. Priority (Critical, High, Medium, Low)
Customer Service Manager	
Name	
Phone	
Email	
Customer Service Manager Backup	
Name	
Phone	
Email	

1.1 Escalation Contact Information

Our goal is to ensure you receive the best possible support from Motorola Solutions Connectivity, Inc. (Motorola). If you feel that your support or maintenance needs are not being met, as a direct Motorola customer, we provide an escalation process for your request to the next Motorola department or manager.

Your initial call should always be to the first department or person on the list above. If, after making this initial contact you still have unresolved issues, there is a stringent escalation process in place. please see below for escalation process.

Note: Upon contract award, you will receive the names, email addresses, and phone numbers of the escalation team members currently assigned to your account.

Table 2 Escalation Contacts

Support Organizations	24x7 Support Number	1st Escalation	2nd Escalation
Network and Security Operations Center (NSOC)	Direct Customers: 1-800-881-4245	Dial the Toll-free 24x7 Support Number to request the On-duty Supervisor NSOC Management: nsocmanagement@motorolasolutions.com	NSOC Manager Email: Phone:
Technical Support Organization (TSO) Tier 3 Support		Technical Support Manager Technical Support Operations Email: Phone:	Sr. Manager Technical Support Operations Email: Phone:
Technical Support Administrators (TSA) Tier 4 Support		Manager Technical Support Administrators Email: Phone:	Sr. Manager Technical Support Administrators Email: Phone:

Section 2

Support Plan Summary

2.1 Introduction

Serving Our Customers' Needs

This Customer Support Plan (CSP) is tailored to the specific needs of Motorola Solutions Connectivity, Inc. (Motorola) Next Generation Core Services (NGCS) customers. Our Service Delivery Team focuses on the health, system performance, and reliability of the services provided in our NGCS portfolio.

A Motorola Customer Service Manager will be the Customer's key point of contact for defining and administering services. The Customer Service Manager's initial responsibility is to update the Customer Support Plan Draft, in collaboration with the Customer, to the finalized CSP that reflects the Customer Contract.

The CSP functions as an operating document that adapts the services described in this document to the Customer's specific solution. Motorola and the Customer will use the CSP to define Customer-specific processes, procedures, solution information, and other relevant support details required to perform the Services set forth in your contract. The final CSP and portions of the Agreement will define the division of responsibilities between the Customer and Motorola.

The Customer Service Manager and Customer will review and amend the CSP on a mutually agreed cadence so the CSP remains current and effective in governing the Advanced Services.

2.2 Service Management Overview

Service Management and open communication is the key to effective service delivery and relationship building. The Motorola Services program offers end-to-end Service Management and includes:

- Customer Service Manager
- Network & Security Operations Center

The Network & Security Operations Center (NSOC) works closely with the NGCS Operations Team to ensure Motorola maintains a holistic view of your service delivery environment.

This Support Plan covers the following locations (to be defined upon award):

Table 3 Site Locations

Site ID	PSAP Name	Address	Phone (24 x 7)	No. of Positions



Section 3

Service Delivery and Support

3.1 Customer Service Manager

Your Customer Service Manager is assigned to work with you to support all aspects of your contracted services. Your Customer Service Manager:

- Works with the Technical Support Center (NSOC) to report on delivery of services to ensure service levels are maintained.
- Works with you and our NSOC to establish and refine policies and procedures to ensure support is consistently delivered.
- Serves as a Point of Escalation when service or support levels are not meeting expectations.
- Serves as the liaison between you and our internal departments for escalated incidents.
- Provides timely and frequent informational updates about progress towards resolving incidents.

3.2 Motorola Network Security Operations Center

The Network Security Operations Center (NSOC) monitors and provides 24x7x365 on-going management of the Motorola NGCS and works closely with the NGCS Operations Team. The NSOC provides:

- Central point of contact to report incidents and submit requests.
- Continuous monitoring of the performance and availability of the solution.
- Creation of alerts based on thresholds and parameters then distributes notifications appropriately.
- Automatic notification emails sent to designated contacts for certain classifications of incidents.

3.3 Reporting Incidents

As the central point of contact to report incidents and submit requests, our NSOC provides 24x7x365 availability to assist with your service needs.

The NSOC is contacted via:

- Telephone 1-800-MSI-HELP (1-800-674-4357), Follow prompts.
- Email: VestaNSOC@motorolasolutions.com – service requests inquiries only, emails are not monitored for an instantaneous response.

- Customer Hub: <https://customerhub.motorolasolutions.com/> – low-priority inquiries or requests only; the Customer Hub is not monitored for an instantaneous response.

NOTE: Critical and High priority incidents **must** be reported via Telephone.

- Product and system technical resources are ready to receive and take action on requests for service.

The NSOC is staffed with technicians trained in the NGCS portfolio of services. Support staff personnel will access the solution remotely to fully understand the incident being reported.

- At a minimum, when reporting an incident, the NSOC will require:
 - Customer name (Site).
 - Caller's name.
 - Caller's contact number (supply alternate call back number).
 - Description of the problem or request.
 - Operational impact of the problem (Priority).
 - When the problem first occurred.
- Upon notification of the incident, the NSOC will supply a case number for reference.

NOTE: For Critical and High severities, the NSOC will continue working with you to begin troubleshooting the reported incident immediately.

- The NSOC will:
 - Open a case and categorize the issue or request.
 - Resolve incidents based on priority.
 - Perform remote analysis to assist in identifying a corrective action plan.
 - Escalate the incident/request to technical or service experts when required.
 - Dispatch Support Engineers where remote corrective actions are not possible.
 - Engage next level management to ensure timely problem resolution.
 - Provide regular status updates for escalated incidents.

3.4 Priority Level and Response Definitions

Response Time – Is defined as the amount of time expired between the time in which the issue is either (a) detected by the NSOC or (b) reported to the NSOC by the Customer to the time that a qualified technician is actively troubleshooting the issue.

Onsite Response Time Coverage – Seven (7) days per week, 24 hours per day, 365 days of the year with a four (4) hour (maximum) response time to have a technician on-site for Critical or High Priority issue related hardware, software, network repair/maintenance issues or events. This includes all Holidays.

Reporting Trouble – The NSOC number is provided to all PSAPs to report issues for NGCS provided 9-1-1 network and equipment. This improves response times whereas the PSAPs do not

need to call two different numbers to report an incident. If the issue that was called in cannot be resolved through our remote diagnostics by the NSOC, then a technician will be on-site within the above stated response times. The NSOC has a call-answering objective of answering 90% of all 9-1-1 calls within 20 seconds.

Incident Time – The period of time during which the service or any service component suffers an Incident. Incident Time will commence when the issue is either (a) detected by the NSOC or (b) reported to the NSOC by the Customer. Incident Time will end upon completion of the repair or restoration of the service or service component. Incident Time will not include downtime attributable to (a) Force Majeure Conditions or (b) scheduled preventive maintenance of which the Customer was notified and to which it consented in advance.

For each reported or alert-generated Critical or High incident, the NSOC will apply a Priority Level classification with an assigned target response time where applicable. This classification provides the means to manage the appropriate response and engagement process.

Table 4 Response Time Definition

Severity	Target Response Time	Description	Communication Interval
Priority 1 (Critical) 24 x 7 x 365	Within 15 minutes	Significant and/or severe degradation of service functionality that impacts inbound call or associated location processing, with no workaround available	Hourly Or as agreed upon with customer
Priority 2 (Major) 24 x 7 x 365	Within 30 minutes	Significant degradation of service functionality where a workaround may be available	Every 2 hours Or as agreed upon with customer
Priority 3 (Minor) Normal Business	Within 8 hours	A minor degradation of service functionality or capacity of inbound call or associated location processing	Daily Or as agreed upon with customer
Priority 4 (Service/Information Request) Normal Business Within 1 Business Day (Excluding Holidays)	Within 1 Business Day	A service request, or degradation of system functional that does not impact inbound call or associated location processing	Updates as needed via Email &/or Motorola Customer Hub

3.5 Customer Hub

The Customer Hub is the user interface into our support structure. The Customer Hub provides direct access to our Incident Management system where you will have access to the same information as our engineers and managers. You may request access to Customer Hub by emailing portal.support@motorolasolutions.com. Include your first and last name, agency name, state, business email, and business phone. The Customer Hub provides the ability to:

- Create low priority cases or requests, provide updates or to obtain status updates for an existing case.
- Obtain status on Service Requests.
- View real-time status of scheduled events (e.g., change requests, service requests, and security patches).

3.6 Support Engineer

While most incidents and service requests are handled remotely, Motorola will dispatch technicians should on-site technical expertise be required.

3.7 Service Maintenance

Motorola will provide the applicable maintenance and repair services to support our Customer for the term of the Service as outlined in the contract and below.

3.8 Maintenance Process

As a leading public safety provider, Motorola understands the importance of how and when maintenance is performed, and of providing proper coordination and notifications. Scheduled maintenance will be handled within our change management process. A change request will be entered in the IT Service Management (ITSM) Tool, ServiceNow, identifying key elements of the change request.

Throughout the Change Management process, the Customer Service Manager is responsible for notifying the PSAP of all planned work that may affect 9-1-1 functionality within a mutually agreed upon period measured in days prior to the event unless an emergency change must be implemented.

Section 4

FCC and State Reporting

If applicable and depending on system configuration, Motorola has implemented policies and procedures in conformance with FCC and state notification and outage reporting rules. To further facilitate company-wide compliance efforts, Motorola trains its employees regarding FCC and state outage notification requirements, as defined in FCC 47 C.F.R. Part 4 and state rules, if any.

In the event of an outage, the designated personnel listed below will be notified by phone call, email, or SMS text message. Consistent with FCC Outage Notification requirements, as soon as possible, but no later than thirty (30) minutes after discovering an outage, network malfunction or higher-level issue that is potentially affecting, i.e., meets the FCC's threshold criteria for notice and report, Motorola will notify the designated personnel for such outages and will convey all available information that may be useful in mitigating the effects of the outage, as well as a name, telephone number, and email address at which Motorola can be reached for follow-up.

4.1 Customer Notification

Motorola will communicate additional material information as it becomes available, but no later than two (2) hours after our initial contact. The additional information will include the nature of the outage, its best-known cause, the geographic scope of the outage, the estimated time for repairs, and any other information that may be useful to the management of the outage.

Customer personnel listed within the Contacts and Notifications chart agree to contact remote sites when there is a service-impacting event. Communication will continue on a regular basis until the event has been resolved.

Table 5 Contacts and Notifications Information

CONTACTS AND NOTIFICATIONS			
SITE NAME	ADDRESS		PHONE NUMBER (24 X 7)
MOTOROLA	NAME	EMAIL	PHONE NUMBER
Critical - System Down notification			

CUSTOMER	NAME/TITLE	EMAIL	PHONE NUMBER
Critical System Down	(Name) (Title)		
Administrative Contact	(Name) (Title)		
911 Authority (Local Govt, Council, Board)	NAME/TITLE	EMAIL	PHONE NUMBER
Authority Contact	(Name) (Title)		
Information Validated:	(Date)		

Note: Incident Notifications are automatically sent through ServiceNow. These notifications are activated whenever an incident is created or modified. To receive these alerts, individuals must be designated as Site Contacts in ServiceNow by the Customer Service Manager.

Section 5

Requesting a Service Change

Service change requests are coordinated directly through the NSOC. To initiate a request, users submit a formal service ticket through our centralized portal, which serves as the primary record for documenting and tracking the modification from inception to completion.

The Customer Service Manager fulfills the role of Change Manager. Information about changes in requirements, network services, application patches, software updates, new service requests, or any other source of change, is tracked in our change management system.

Motorola's service and engineering staff will assess and identify the potential impact, risk, timeline, and any costs (if applicable) associated with functional change, hardware or component additions, integration to additional systems/networks, etc.

The change management process ensures that all service change requests to the NGCS services are properly documented, reviewed, and all stakeholders are notified prior to implementation.

5.1 Requesting a GIS Change Impacting Call Routing

If Location Service is purchased, a GIS change request is also coordinated through the NSOC by the Customer Service Manager. A GIS Change Management Request form is initiated by completing the Change Management Request Form and submitting it to your Customer Service Manager. The Customer Service Manager will submit it to the NSOC and a ticket will be created to get the request on the agenda for the Change Approval Board. Once the GIS change has been reviewed and approved, notification of approval will be sent back through the Customer Service Manager for communication to you. The requested GIS change may then be pushed to Spatial Central within the normal change window of the Change Management Process.

Section 6

Conditions and Exclusions

6.1 Conditions

Motorola ensures the optimal performance of the Service. In order to provide a consistent level of quality services, the following conditions and limitations apply:

- On-site intervention requires Customer to provide site access.
- Remote monitoring, troubleshooting and restoration requires that the Customer provide direct unencumbered remote access 24x7x365 to all applicable locations and equipment.

6.2 Exclusions

Motorola's service and support obligations hereunder will not apply to any Motorola supported software or hardware if correction of an error, adjustment, repair, or parts replacement is required because of:

- Accident, neglect, tampering, misuse, improper/insufficient grounding, failure of electric power, failure of Customer and/or others to provide appropriate environmental conditions, relocation of hardware or software, or causes other than ordinary use.
- Repair or alteration, or attempted repair or alteration of any supported hardware and/or software by Customer or others, unless otherwise approved in writing by Motorola.
- Connection of another machine, device, application, or interface to Motorola supported equipment (hardware and/or software) by Customer or others, which has caused damage to Motorola supported equipment.
- Damage or destruction caused by natural or man-made acts or disasters.
- Failure or degradation in performance of Motorola's supported equipment (hardware and/or software) due to the installation of another machine, device, application, or interface not specifically certified and approved by Motorola for use in Customer's environment.
- The operation of the software in a manner other than that currently specified in the applicable product documentation.
- The failure of the Customer to provide suitably qualified and adequately trained operating and maintenance staff.
- Incompatible or faulty Customer hardware and/or software interfaces.
- Modifications made without Motorola's written approval to the OS, network, hardware or software environment or software applications.

Further, support described herein does not include cosmetic repairs, refurbishment, furnishing consumables, supplies or accessories, making accessory changes, the performance of preventive maintenance or system administration, or adding additional devices or software applications.

DRAFT