



RFP # XYZ110001010

Response to State of Nebraska Solicitation No. 202691101 — Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS)

Contents

VOLUME 1: Corporate Overview	1
A. BIDDER IDENTIFICATION AND INFORMATION	1
B. FINANCIAL STATEMENTS	1
Financial Overview and Organizational Description	1
Banking Reference	2
Litigation and Financial Disclosure	3
C. CHANGE OF OWNERSHIP	3
Completed Ownership Transaction – July 9, 2024	3
Anticipated Changes Within 12 Months of April 15, 2026	4
D. OFFICE LOCATION	4
E. RELATIONSHIPS WITH THE STATE	5
Pre-RFP Engagement – January 2025	5
F. BIDDER'S EMPLOYEE RELATIONS TO STATE	5
G. CONTRACT PERFORMANCE	6
Terminations for Default (Past 10 Years)	6
Terminations for Convenience (Past 5 Years)	6
H. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE	6
Corporate Experience Summary Matrix	6
Project Narrative 1: Indiana (IN911) Statewide ESInet and NGCS PRIME VENDOR	7
Project Narrative 2: Alabama (ANGEN 2.0) Statewide ESInet and NGCS PRIME VENDOR	7
Project Narrative 3: New Hampshire – Statewide ESInet and NGCS PRIME VENDOR	8
I. SUMMARY OF BIDDER'S PROPOSED PERSONNEL / MANAGEMENT APPROACH	9
Project Team Summary	10
Management Approach and Reporting Structure	11
J. SUBCONTRACTORS	12
VOLUME 2: Response to Scope of Work	14
2.1 Executive Summary and Project Overview	14
2.1.1 Nebraska-Specific Commitments	14
2.2 ESInet Architecture and Design Approach (§B.1, §E.1)	15
2.2.1 Architecture Overview and Geographic Redundancy (§E.1.1)	15

2.2.2 IPv4 and IPv6 Dual-Stack (§E.1.1).....	16
2.2.3 Quality of Service (§E.1.4).....	16
2.2.4 SIP Signaling and Media Security (§E.1.1)	18
2.2.5 Points of Interconnection and Peering Interfaces (§E.1.2).....	18
2.2.6 Dual-Manufacturer Routers (§E.1.5.2)	18
2.2.7 Bandwidth Provisioning and Capacity (§E.1.4.2).....	18
2.2.8 MEVO Continuity of Service (§E.1.5).....	19
2.3 NGCS Approach (§B.2, §E.2)	19
2.3.1 NGCS Functional Elements (§E.2.1, §E.2.2)	19
2.3.2 Additional NGCS Components (§E.2.3)	20
2.3.3 i3 v2 and v3 Dual-Version Support (§B.3).....	20
2.3.4 Text-to-911 and TCC (§E.2.4.2.3).....	20
2.3.5 Latency and Interface Documentation.....	20
2.4 GIS and Location-Based Routing Approach (§E.3)	20
2.4.1 NENA-STA-006.2-2022 Conformance and Required Layers (§E.3.1)	21
2.4.2 Five-Minute Routing Update SLA (§E.3.1).....	22
2.4.3 GeoComm Partnership: Spatial Interface and End-User Validation (§E.3.1.2)	23
2.4.4 PIDF-LO, Change Tracking, and Export Formats (§E.3.1).....	23
2.5 Call Flow and Media Session Handling Approach (§B.4, §E.2.4)	24
2.5.1 NENA i3 Call Flow Sequence (§E.2.4.1).....	24
2.5.2 SIP Header Preservation (§E.2.4.1).....	24
2.5.3 Real-Time Multimedia (§E.2.4.2).....	24
2.5.4 PSAP Transfer with Metadata Preservation (§E.2.4.1)	25
2.6 Security, Privacy, and Trust Approach (§B.5, §E.4).....	25
2.6.1 NENA Trust Model and Boundary Enforcement (§E.4.1.2, §E.4.2.4).....	25
2.6.2 Encryption and Key Management (§E.4.4)	25
2.6.3 Dedicated Security Architect (§E.4.1.1)	26
2.6.4 Incident Response and Penetration Testing (§E.4.1.3, §E.4.7).....	26
2.6.5 Nebraska Revised Statute 86-125 Compliance.....	26
2.7 Logging, Reporting, and Call Detail Records Approach (§B.6, §E.5)	26
2.7.1 Call Detail Records and Log Fields (§E.5.1)	26
2.7.2 Secure Storage and Access Control (§E.5.2)	27
2.7.3 Export Formats and Operational Reports (§E.5.3).....	27
2.7.4 Data Interface to PSC Analytics Engine (§E.5.4).....	27
2.7.5 Separately Awarded State Logging Contractor	27

2.8 Interoperability, Testing, and Acceptance Approach (§B.7).....	27
2.8.1 Conformance and Interoperability Testing (§B.7).....	28
2.8.2 Independent Third-Party V&V (§C.5).....	28
2.8.3 Documentation Package (§B.7)	28
2.9 Service Management Framework (§E.8)	28
2.9.1 Service Management Plan (§8.1.1).....	29
2.9.2 Service Level Agreement (§8.1.2)	30
2.9.2.1 Help Desk and Response KPIs.....	31
2.9.3 Compliance and Risk Management (§8.1.3).....	31
2.9.4 Monthly Project Review and Compliance (§8.1.4).....	31
2.9.5 Continuity and Resilience (§8.2).....	32
2.9.5.1 Availability (§8.2.1)	32
2.9.5.2 Continuity of Operations Plan (§8.2.2)	32
2.9.5.3 Disaster Recovery (§8.2.3)	32
2.9.6 Operations Centers and Support (§8.3).....	33
2.9.6.1 Network Operations Center (§8.3.1).....	33
2.9.6.2 Security Operations Center (§8.3.2)	33
2.9.6.3 Help Desk (§8.3.3)	33
2.9.6.4 Customer Support Services (§8.3.4)	34
2.9.7 Monitoring and Event Management (§8.4).....	34
2.9.7.1 Alarm Categories.....	34
2.9.8 Change, Maintenance, and Release Management (§8.5).....	35
2.9.8.1 Change Management (§8.5.1)	35
2.9.8.2 Security Considerations in Change Management (§8.5.1.1).....	35
2.9.8.3 Scheduled Maintenance Process (§8.5.2)	35
2.9.8.4 Software Development Process (§8.5.3)	35
2.9.8.5 Software Updates and Improvements (§8.5.4)	36
2.9.8.6 Implementation-Phase Contingency and Rollback (§C.4.a).....	36
2.9.9 Spares and Inventory (§8.6).....	36
2.10 NENA-STA-010.3f-2021 Conformance Disclosure Table (§B.3).....	38
2.11 Value-Add and Optional Services: Call Handling Equipment (§9)	56
2.11.1 INDIGITAL's CHE Partnership Approach (§E.9.1)	56
2.11.2 Hosted CHE Capability Description (§E.9.1)	56

2.11.3 Transition Path for Nebraska PSAPs (§E.9.1).....	57
2.11.4 ESInet and NGCS Backup System (§9.2).....	57
VOLUME 3: Work Plan	59
3.1 Project Management Approach (§E.6)	59
3.1.1 Governance Structure.....	59
3.1.2 Project Manager	59
3.1.3 Preliminary Project Management Plan (PMP).....	60
3.1.4 Scope, Schedule, and Budget Control	61
3.1.5 Risk and Issue Management	61
3.1.6 Stakeholder Communications and Status Reporting.....	62
3.1.7 Key Personnel and Staffing.....	62
3.2 Implementation, Transition, and Cutover Plan (§E.6)	63
Element 1 – Implementation Plan	64
3.2.1 Implementation Methodology and Phasing	64
3.2.2 IP Routing Plan and Governance.....	65
3.2.3 NGCS and ESInet Functional Integration.....	65
Element 2 – Transition Plan	65
3.2.4 OSP Interface Transitions and Incumbent Transition Strategy	65
3.2.5 Parallel Operations Model.....	66
3.2.6 Standards-Based Interconnection Layer	66
3.2.7 Contingency: Third-Party Interconnection Bridge (Sinch).....	67
3.2.8 Traffic Control and Routing Policy During Transition.....	67
3.2.9 End-to-End Testing and Live Traffic Validation.....	67
3.2.10 NOC and SOC Coverage Throughout.....	68
3.2.11 Southeast Region Independence (Q&A #5).....	68
3.2.12 System Testing During Transition	68
3.2.13 Parallel Operation and Rollback	68
3.2.14 Contingency and Rollback Procedures.....	69
3.2.15 Risks, Dependencies, and Incumbent Coordination	69
Element 3 – Cutover Plan	69
3.2.16 Site Surveys and Installation (Q&A #16)	69
3.2.17 Software Upgrade and Change Methodology (Q&A #36)	70

3.2.18 Master Project Schedule and Milestone Matrix.....	70
3.3 Testing and Acceptance Plan (§C.5)	76
3.3.1 Test Environment, Facilities, and Equipment.....	77
3.3.2 Test Configurations and Thresholds.....	77
3.3.3 Simulators and Test-Call Processes	77
3.3.4 Test Methodology: TP/TF/RTP/RTF/NA	78
3.3.5 System Testing Coverage	78
3.3.6 State Participation Rights	80
3.3.7 Independent Validation and Verification (IV&V).....	80
3.4 Training Plan (§E.7)	80
3.4.1 PSAP Operator Training	81
3.4.2 System Administrator Training.....	81
3.4.3 Commission Staff Training	81
3.4.4 Training Deliverables	81
3.4.4.1 Training Plan and Sample Materials (RFP §7.8).....	82
3.4.4.2 Train-the-Trainer (TtT) Curriculum (RFP §7.5)	82
3.4.4.3 PSAP Operator Quick-Start Guide	82
3.4.4.4 PSAP Operator Full Reference Manual.....	82
3.4.4.5 System Administrator Manual.....	82
3.4.4.6 Commission Staff Oversight and Reporting Guide	82
3.4.4.7 Emergency Procedures Runbook.....	82
3.4.4.8 Comprehension Testing and Certification Materials (RFP §7.7)	83
3.4.4.9 Post-Deployment Training Materials (RFP §7.6)	83
3.4.4.10 Application-Specific Training Materials.....	83
3.4.4.11 Scheduling and Logistics Documentation (RFP §7.4)	83
VOLUME 4: Response To Technical Requirements	84
4.1 ESInet Technical Narrative (§E.1)	84
4.1.1 Architecture and Topology (§E.1.1)	84
4.1.1.1 Multi-Tenant and Interconnect Design	84
4.1.1.2 Redundancy and Failover.....	85
4.1.1.3 SIP, TLS, and Media Security	85
4.1.1.4 ESInet Architecture Diagrams	85

4.1.2 External and PSAP Connectivity (§E.1.2).....	88
4.1.2.1 Originating Service Provider (OSP) Connections (§E.1.2.1).....	88
4.1.2.2 PSAP Connections (§E.1.2.2).....	88
4.1.3 Legacy Interoperability (§E.1.3).....	88
4.1.4 Network Performance (§E.1.4).....	89
4.1.4.1 QoS and Traffic Prioritization	89
4.1.4.2 Bandwidth Provisioning (§E.1.4.2)	89
4.1.4.3 Network Time (§E.1.4.6).....	89
4.1.5 Resilience and Service Levels (§E.1.5)	89
4.1.5.1 Availability (§E.1.5.1)	89
4.1.5.2 Router Diversity and Reliability (§E.1.5.2)	89
4.1.5.3 Multivendor diversity:.....	90
4.1.5.4 Cisco.....	90
4.1.5.5 Arista	90
4.1.5.6 Fortinet.....	90
4.1.6 Operations and Management (§E.1.6).....	90
4.1.6.1 Network Operations Center (§E.1.6.1)	90
4.1.6.2 Maintenance Windows (§E.1.6.2).....	91
4.1.6.3 Implementation Details and Port Mapping (§E.1.7).....	91
4.1.7 ESInet Interconnection with Neighboring States (§E.1.1.2).....	91
4.2 NGCS Technical Narrative (§E.2)	92
4.2.1 Architecture and Data Center Deployment (§E.2).....	92
4.2.1.1 Failover and State Management.....	92
4.2.2 Edge Security and Ingress (§E.2.1)	92
4.2.2.1 Border Control Function (BCF, §E.2.1.1).....	92
4.2.2.2 STIR/SHAKEN Support (§E.2.1.2).....	93
4.2.2.3 Security Mechanisms (§E.2.1.3).....	93
4.2.3 Core Routing and Location (§E.2.2)	93
4.2.3.1 Emergency Services Routing Proxy (ESRP, §E.2.2.1)	93
4.2.3.2 Policy Store (§E.2.2.1.1)	93
4.2.3.3 Location Information Server – LIS Interface (§E.2.2.2)	93

4.2.3.4 Location Database (LDB, §E.2.2.3)	94
4.2.3.5 ECRF and LVF (§E.2.2.4)	94
4.2.3.6 Forest Guide (§E.2.2.5)	94
4.2.3.7 Service/Agency Locator (SAL, §E.2.2.6)	94
4.2.4 Data and Enrichment (§E.2.3)	94
4.2.4.1 Additional Data Repository (ADR, §E.2.3.1)	94
4.2.5 Call Flow and Media Handling (§E.2.4)	95
4.2.5.1 i3 Call Flows and SIP Header Preservation (§E.2.4.1)	95
4.2.5.2 Multimedia Support (§E.2.4.2.1)	96
4.2.5.3 Media Quality of Service (§E.2.4.2)	96
4.2.5.4 Interactive Multimedia Response Service (IMRS, §E.2.4.3)	96
4.2.5.5 Bridge (§E.2.4.4)	96
4.2.6 Legacy Bridging (§E.2.5)	96
4.2.7 Outgoing Call Interface Function (OCIF) (§E.2.5.1)	96
4.3 GIS and Location Technical Narrative (§E.3)	97
4.3.1 Data Management and GIS Foundation (§E.3.1)	98
4.3.1.1 NENA GIS Data Model Conformance	98
4.3.1.2 Data Integrity Gateway (DIG) & GeoComm Spatial Interface (§3.1.2)	98
4.3.1.3 GeoComm GIS Data Hub	98
4.3.1.4 Maintain – Operational Definition	99
4.3.1.5 Location Integrity Oversight Service (LIOS)	100
4.3.1.6 Data Governance and Provisioning	100
4.3.2 Location Conveyance (§E.3.1)	100
4.3.3 Core Data Services (§E.3.2)	100
4.3.3.1 Mapping Data Service (MDS, §E.3.2.1)	100
4.3.3.2 MSAG Conversion Service (MCS, §E.3.2.2)	100
4.3.3.3 Geocode Conversion Service (GCS, §E.3.2.3)	101
4.3.4 PSAP-Facing Services (§E.3.3)	101
4.3.4.1 PSAP Mapping Service (§E.3.3.1)	101
4.3.4.2 Map Discrepancy Reporting (§E.3.3.2)	101
4.3.5 External GIS Integrations (§E.3.4)	101

4.4 Security Technical Narrative (§E.4).....	101
4.4.1 Security Management and Process Control (§E.4.1)	102
4.4.1.1 Personnel Roles and Responsibilities (§E.4.1.1).....	102
4.4.1.2 Personnel Roles and Responsibilities – Required Security Roles Matrix (§E.4.1.1)	103
4.4.1.3 Nebraska NG911 ESInet/NGCS – Security Roles RACI Matrix	105
4.4.2 Incident Response Plans (§E.4.1.3.1)	110
4.4.2.1 Cybersecurity Incident Response Plan (CIRP)	110
4.4.2.2 Phase 1: Preparation	110
4.4.2.3 Phase 2: Detection and Analysis.....	111
4.4.2.4 Phase 3: Containment, Eradication, and Recovery	112
4.4.2.5 Phase 4: Post-Incident Activity	113
4.4.2.6 Detection Capabilities and Processes.....	113
4.4.2.7 Training and Exercise Evidence.....	114
4.4.2.8 Business Continuity (BC) Plan.....	114
4.4.2.9 Disaster Recovery (DR) Plan.....	115
4.4.2.10 Plan Maintenance and Accessibility Controls	115
4.4.2.11 Review and Test Cadence	116
4.4.2.12 Containment and Recovery Playbooks	116
4.4.2.13 Malware and Ransomware Playbook.....	116
4.4.2.14 Denial of Service (DDoS/TDoS) Playbook.....	117
4.4.2.15 Critical Service Outage Playbook.....	117
4.4.2.16 External Assistance Procedures.....	118
4.4.3 Authorization and Data Rights Management (§E.4.1.4).....	118
4.4.3.1 Authorization Architecture.....	119
4.4.3.2 Policy Naming Conventions and Registry Usage	120
4.4.3.3 Action Model.....	120
4.4.3.4 Example XACML Policy Sets	121
4.4.3.5 JWS Packaging and Validation	122
4.4.3.6 Data Rights Management Procedures.....	123
4.4.3.7 Policy Lifecycle Controls.....	123

4.4.3.8 Logging and Auditability	124
4.4.3.9 Performance and Availability Targets.....	124
4.4.4 Identity Management and PKI (§E.4.1.2).....	125
4.4.4.1 Federated SSO and External Identity Providers (§E.4.3).....	127
4.4.5 Information System Infrastructure and Management (§E.4.2).....	127
4.4.5.1 Device Inventory (§E.4.2.1).....	127
4.4.5.2 Patching and Update Management (§E.4.2.2)	127
4.4.5.3 Network Segmentation and Traffic Separation (§E.4.2.3)	127
4.4.5.4 Network Boundary Protection (§E.4.2.4)	127
4.4.6 Cryptography (§E.4.4)	128
4.4.7 Integrity Protection (§E.4.5).....	128
4.4.7.1 JSON Web Signatures (§E.4.5.1)	128
4.4.8 Security Monitoring, Detection, and Alerting (§E.4.8).....	128
4.4.8.1 Security Event Logging and Continuous Monitoring (§E.4.8.1)	128
4.4.8.2 Time Synchronization (§E.4.8.1.1).....	129
4.4.8.3 Denial of Service and Telephony Denial of Service Mitigation (§E.4.8.2)	129
4.4.9 Neb. Rev. Stat. §86-125 Compliance	129
4.4.10 Information Privacy (§E.4.6).....	130
4.4.10.1 Access Controls for Sensitive Data	130
4.4.10.2 Neb. Rev. Stat. and Federal Alignment	130
4.4.11 Security Assessment and Audit (§E.4.7)	130
4.4.11.1 Penetration Testing	130
4.4.11.2 Vulnerability Scanning	131
4.4.11.3 External Compliance Audits	131
4.4.11.4 Internal Audit Program.....	131
4.4.11.5 Risk Assessment.....	131
4.4.11.6 Assessment and Audit Documentation (§E.4.7.1).....	131
4.4.12 Intrusion Detection and Prevention (§E.4.8.3)	132
4.4.12.1 Deployment Architecture	132
4.4.12.2 Detection Capabilities.....	132

4.4.12.3 Response and Integration.....	132
4.4.12.4 Tuning and Maintenance	132
4.4.13 DNS Security (§E.4.9)	133
4.4.13.1 DNS Architecture and Resilience	133
4.4.13.2 DNS Threat Mitigation	133
4.4.13.3 Integration with NG911 Services	133
4.5 Standards Conformance Narrative (§B.3)	133
4.6 Router Diversity and Network Redundancy (§E.1.5)	135
4.6.1 Dual-Manufacturer Router Architecture	136
4.6.1.1 Cisco.....	136
4.6.1.2 Arista	136
4.6.1.3 Fortinet	136
4.6.2 Three-Dimensional Diversity	137
4.6.3 FCC Report and Order 13-158 Conformance.....	137
4.7 In-State Data Center Response.....	137
4.7.1 Proposed Data Center Architecture	137
4.7.2 Why In-State Infrastructure Matters for Nebraska	137
4.7.3 Evaluation Scoring Impact	138
4.8 Reporting Services Requirements (§E.5)	138
4.8.1 Reporting and Data Collection Requirements (§E.5.1)	138
4.8.2 Logging Service (§E.5.2)	139
4.8.3 i3 Logging and Reporting Requirements (§E.5.3)	139
4.8.4 Functional Element Reporting (§E.5.4)	139
4.8.5 Monitoring, Outages, Failover, Trouble Tickets, and Escalation (§E.5.5)	141
4.8.6 Maintenance and Configuration Reports (§E.5.6).....	141
4.8.7 Discrepancy Reporting (§E.5.7)	142
4.9 Use Case Narratives (§E.10).....	143
4.9.1 Normal Call Flow: Wireless 911 Call, Metro Region (§E.10.1)	144
4.9.1.1 Step 1: Call Origination and OSP Handoff.....	144
4.9.1.2 Step 2: BCF Admission and Security Enforcement.	144
4.9.1.3 Step 3: ESRP Policy Evaluation.	144
4.9.1.4 Step 4: ECRF Location-Based Routing.....	144
4.9.1.5 Step 5: ESRP Call Routing to PSAP.	145

4.9.1.6 Step 6: PSAP Call Delivery and Answer.	145
4.9.2 Abnormal Call Flow: Location Resolution Failure with Default Routing (§E.10.2)....	145
4.9.2.1 Step 1: SIP INVITE with Incomplete Location.	145
4.9.2.2 Step 2: BCF Admission and LVF Validation Attempt.	145
4.9.2.3 Step 3: ECRF Default Routing.	146
4.9.2.4 Step 4: PSAP Delivery with Location Warning.	146
4.9.3 Failure Scenario: ESInet Node Failure with Automatic Failover (§E.10.1).....	146
4.9.3.1 T+0: Power Loss at Primary Data Center.	146
4.9.3.2 T+3 seconds: Health Check Failure Detection.	146
4.9.3.3 T+4 seconds: Active-Active Failover Activation.....	147
4.9.3.4 T+5 seconds: RTO Achievement.	147
4.9.3.5 T+15 minutes: NSOC Notification and Incident Response.	147
4.9.3.6 T+ongoing: Redundancy Restoration.....	147
Appendix 4-A: ESInet and NGCS Port Mapping	147
Appendix 4-B: FIPS 140-3 Cryptographic Module Inventory	152
Appendix 4-C: Cross-Reference to Volumes 2 and 3	152
§E.6 – Installation (Volume 3, Section 3.2)	152
§E.7 – Training (Volume 3, Section 3.4)	152
§E.8 – Operations and Service Management (Volume 2, Section 2.3)	152
§E.9 – Project Management (Volume 3, Section 3.1)	153
VOLUME 5: Terms and Conditions	154
5.1 TERMS ACCEPTANCE / EXCEPTION TABLE.....	154
5.1.1 Deliverable Approval Process.....	154
5.1.1.1 Submission and Notification	155
5.1.1.2 Commission Review Period.....	155
5.1.1.3 Acceptance and Rejection.....	155
5.1.1.4 Escalation and Dispute Resolution	155
5.1.1.5 Single Point of Contact	156
5.2 LICENSE, USER AGREEMENTS, AND SLAS.....	156
Appendix A: Resumes.....	157

VOLUME 1: Corporate Overview

A. BIDDER IDENTIFICATION AND INFORMATION

Full Legal Business Name	Communications Venture Corp d/b/a INDIGITAL
Headquarters Address	1616 Directors Row, Fort Wayne, IN 46808
Telephone	877-469-2010
Federal Tax ID	35-1957521
Unique Entity Identifier	J6JSAK2TV3D3
Entity Organization Type	Corporation
State of Incorporation	Indiana
Year First Organized	1995
Primary Contact (Proposal)	Sandi Stroud - VP Public Safety - 651-302-8602
Authorized Signatory	Jeff Humbarger - CFO

B. FINANCIAL STATEMENTS

INDIGITAL fully complies with this requirement. As a privately held company, INDIGITAL does not publish audited financial statements. The following narrative and supporting data provide the information required under this provision, consistent with the RFP's stated alternative for non-public firms.

Financial Overview and Organizational Description

INDIGITAL, operating as Communications Venture Corp d/b/a INDIGITAL under parent INDIGITAL Holdings, Inc., is a financially stable, privately held company with over 30 years of continuous operation exclusively in the public safety communications sector. INDIGITAL's revenue is derived entirely from the design, deployment, and long-term operation of Next

Generation 9-1-1 (NG911) infrastructure for state and local government clients. The company pursues no commercial telecommunications work, no defense contracts, and no service lines outside emergency communications.

INDIGITAL's most recent full-year consolidated financial results (year ending December 31, 2024, audited by independent public accountants, clean opinion with no going-concern qualification) demonstrates the following:

Financial Metric	Value (FY 2024, Audited)
Total Revenue	\$71.1 million
EBITDA	\$8.7 million (positive; company is operationally profitable)
Net Loss	\$(3.57) million – entirely attributable to \$6.3M in non-cash acquisition-related amortization of intangibles (\$111M goodwill/intangibles recorded at acquisition). Not indicative of operational performance.
Total Assets	\$157.7 million
Stockholders' Equity	\$72.5 million
Audit Opinion	Unqualified (clean) no going-concern language

The net loss reported for 2024 reflects the stub period of July 9–December 31, 2024, following the Novacap acquisition. The non-cash amortization charge arises from the purchase price allocation of \$111 million in goodwill and identified intangible assets at acquisition, a standard accounting treatment for privately held companies acquired at a premium to book value. INDIGITAL's operating cash flows and EBITDA are positive, confirming the company's operational and financial stability. No-going-concern qualification was issued.

INDIGITAL employs more than 150 professionals, all dedicated exclusively to public safety communications. The company holds active multi-year contracts across 26 states, with the largest single engagement – the State of Indiana – currently generating approximately \$1.4 million per month in recurring revenue under a contract running through December 2028.

Banking Reference

INDIGITAL's primary banking relationships are with Royal Bank of Canada (RBC) and Old National Bank (ONB). In connection with the July 2024 acquisition, RBC extended a \$35 million term loan (at variable SOFR-based interest, maturing July 9, 2028) and a \$10 million revolving credit facility (\$6 million drawn on December 31, 2024, current balance of \$2 million). This relationship reflects the confidence of a major institutional lender in INDIGITAL's revenue base,

client contract portfolio, and long-term financial stability. INDIGITAL's deposit relationship is with Old National Bank. This relationship has been in place since 2014.

Litigation and Financial Disclosure

INDIGITAL discloses the following with respect to pending litigation, bankruptcy proceedings, and material financial events:

No pending litigation, suits, or claims related to the services INDIGITAL provides exist as of the proposal due date. INDIGITAL has not experienced any bankruptcy filing, insolvency proceedings, or material financial reversal in its operating history.

The July 9, 2024, acquisition of Communications Venture Corp by Novacap through newly formed INDIGITAL Holdings, Inc. constitutes a material ownership transaction. This event is disclosed fully in Section 1-C of this proposal. The acquisition was completed in the ordinary course of private equity investment, resulting in no operational disruption, no change in key personnel, and no alteration to existing client contracts. INDIGITAL considers this a reportable event under the RFP's financial disclosure provision and discloses it proactively.

C. CHANGE OF OWNERSHIP

INDIGITAL fully complies with this requirement. In the interest of full transparency, INDIGITAL discloses the following completed ownership event and affirms its current ownership structure.

Completed Ownership Transaction — July 9, 2024

On July 9, 2024, Novacap, a leading Canadian-based private equity firm, completed the acquisition of 100% of the equity interest of Communications Venture Corporation through newly formed INDIGITAL Holdings, Inc. The total purchase consideration was approximately \$115.6 million, comprised of \$97.8 million in cash, \$16.4 million in rollover equity from continuing management and investors, and \$1.3 million in contingent consideration. Following the transaction, INDIGITAL's ownership and governance structure are as follows:

Entity	Role / Description
Novacap	Ultimate parent and controlling investors. Montreal-based PE firm with \$10B+ AUM. Provided acquisition financing and holds majority economic interest through INDIGITAL Holdings.
INDIGITAL Holdings, Inc.	Newly formed parent holding company created to facilitate the acquisition. Consolidating entity for financial reporting.
INDIGITAL US Holdings, Inc.	Intermediate holding entity.
Communications Venture Corp (d/b/a INDIGITAL)	Primary operating entity. Unchanged — same legal entity, same contracts, same personnel, same EIN (35-1957521), same HQ address

Entity	Role / Description
	(1616 Directors Row, Fort Wayne, IN). This is the entity submitting this proposal.
Ryan Public Safety Solutions	Sister operating subsidiary under INDIGITAL US Holdings.

The July 2024 acquisition produced no change in INDIGITAL's operational performance, key personnel, client contracts, or service delivery model. No existing contract was modified, transferred, or renegotiated as a result of the transaction. All service level commitments to current clients have been continuously met.

Anticipated Changes Within 12 Months of April 15, 2026

As a privately held company, INDIGITAL acknowledges that ownership transitions are evaluated on an ongoing basis and ownership structures may evolve as part of normal business operations. Should any change in ownership or control occur, INDIGITAL commits to providing prompt notification to the Commission in accordance with contract requirements. As with the Novacap acquisition, no material changes in INDIGITAL's ability to meet the contractual and operational commitments to Nebraska would occur.

D. OFFICE LOCATION

The INDIGITAL office with primary responsibility for performance under this contract is:

Primary Office	INDIGITAL National Headquarters 1616 Directors Row Fort Wayne, IN 46808 877-469-2010
Nebraska Operations	INDIGITAL will commit to dedicated state resources for this project. Location TBD upon award.

INDIGITAL's service model is built on deploying in-state personnel for every project engagement. Market Managers and field coordinators are embedded in the states they serve, bringing direct knowledge of each agency's operational environment, personnel, and technical infrastructure. These in-state resources are former telecommunicators and emergency communications professionals who bring prior public safety and dispatch experience to every client relationship.

For Nebraska, INDIGITAL will designate a dedicated Nebraska Market Manager/Service Manager who will be responsible for 24-hour-per-day access to the INDIGITAL NSOC and executive management, day-to-day coordination with the Nebraska PSC Contract Administrator, and direct liaison with individual PSAP agencies across all 7 regions. There will also be 4 dedicated service technicians in state to ensure that response SLAs are met.

E. RELATIONSHIPS WITH THE STATE

INDIGITAL fully complies with this requirement. INDIGITAL discloses the following prior dealings with the State of Nebraska within the 10-year period preceding the proposal due date of April 15, 2026.

Pre-RFP Engagement — January 2025

On or around January 8, 2025, INDIGITAL representatives met with David Sankey, Nebraska 911 Coordinator, Nebraska Public Service Commission. The purpose of the meeting was to discuss Nebraska's planned NG911 procurement, current ESInet infrastructure challenges, and INDIGITAL's capability to serve as a statewide NG911 provider. Topics discussed included Nebraska's in-state data center requirements, the existing Lumen ESInet architecture, and the Commission's evaluation approach for the forthcoming solicitation.

Following the January 2025 meeting, INDIGITAL provided Mr. Sankey with reference materials including a draft Statement of Work, a Market Manager role description, and state operational reporting templates. INDIGITAL subsequently participated in Nebraska 911 activities including board meetings and relevant NENA conferences consistent with standard pre-solicitation industry engagement.

INDIGITAL attended and participated in the mandatory Solicitation Conference for RFP 202691101 on March 2, 2026, consistent with solicitation requirements.

Contact	Detail
State Contact	David Sankey, Nebraska 911 Coordinator, Nebraska Public Service Commission
Contact Information	dave.sankey@nebraska.gov 402-471-3101
Nature of Contact	Pre-solicitation informational meeting: reference materials provided; 911 board meeting and NENA conference participation
Prior Nebraska Contracts	INDIGITAL has not held any contracts with the State of Nebraska or any Nebraska state agency within the 10-year period preceding the proposal due date of April 15, 2026.

F. BIDDER'S EMPLOYEE RELATIONS TO STATE

No party named INDIGITAL's solicitation response is or was an employee of the State of Nebraska within the past six (6) months. INDIGITAL so declares.

No employee of any agency of the State of Nebraska is employed by INDIGITAL or serves as a subcontractor to INDIGITAL as of the proposal due date. INDIGITAL so declares.

G. CONTRACT PERFORMANCE

Terminations for Default (Past 10 Years)

INDIGITAL has not experienced any contract termination for default during the past ten (10) years. INDIGITAL so declares.

Terminations for Convenience (Past 5 Years)

INDIGITAL has not experienced any contract termination for convenience during the past five (5) years. INDIGITAL so declares.

H. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

INDIGITAL is the nation's pioneer in statewide NG911 infrastructure, operating across more than 26 states at county, regional, and statewide scale. The following summary matrix identifies our most directly comparable prior engagements, followed by three detailed narrative descriptions. All three featured engagements were performed as the prime vendor.

Corporate Experience Summary Matrix

State / Client	Contract Period	Role	PSAPs Served	Scope
Indiana (IN911)	Jun 2006 – Dec 2028	Prime	118 PSAPs / 92 Counties	ESInet, NGCS, CHE, GIS, T2911, MEVO, Security
Alabama (ANGEN 2.0)	Jan 2017 – Dec 2027	Prime	All AL PSAPs / Statewide	ESInet, NGCS, MEVO, GIS, Translation, Security
New Hampshire	Oct 2015 – Oct 2027	Prime	Statewide	ESInet, NGCS, TCC, NG-ALI, MEVO, Security
Vermont	Mar 2019 – Apr 2028	Prime	Statewide	ESInet, NGCS, GIS, MEVO
Rhode Island	Jun 2022 – Jul 2028	Prime	Statewide	ESInet, NGCS, GIS, MEVO, i3v3
Michigan (w/ PFN)	Ongoing	Prime / NGCS Partner	All MI Counties	NGCS – ESRP, ECRF, LVF, PRF, logging, security
Motorola Solutions (National)	Ongoing	Prime Subcontractor	National footprint	27M+ calls/year; OSP delivery, SBCs, BCF, ESRP, NSOC

Project Narrative 1: Indiana (IN911) Statewide ESInet and NGCS | PRIME VENDOR

Client	Indiana 911 State Board
INDIGITAL Role	Prime Contractor
Period of Performance	June 2006 – December 2028 (active; includes multiple renewal terms)
PSAPs Served	120 PSAPs across 92 Indiana counties; INDIGITAL serves as Statewide Service Provider (SSP) for 79 PSAPs on NGCS; MEVO Anywhere and Texty services at all 120 PSAPs statewide
Contract Value	Approximately \$15.8 million annually (current term)
Uptime / SLA Performance	99.999% availability – maintained across multiple contract years
Contact Details	Jeff Schemmer, jschemmer@in911.net 317-234-2507

Indiana represents INDIGITAL's flagship engagement and the most direct parallel to Nebraska Solicitation #202691101. Indiana was one of the first states in the nation to deploy a statewide ESInet – a milestone INDIGITAL delivered. Today, INDIGITAL serves all 92 Indiana counties and 118 PSAPs, providing ESInet, NGCS (ESRP, ECRF, LVF, PRF, BCF), Text-to-911 (pioneered in 2013–2014 under INDIGITAL's leadership), Managed Emergency Voice Operations (MEVO) for PSAP continuity, hosted call handling, GIS integration, cybersecurity services, training, and ongoing operational support through the 24x7x365 National Service Operations Center (NSOC).

Indiana launched Text-from-911 in 2013 and Text-to-911 in 2014 under INDIGITAL's leadership – well before most states had a defined transition path. All primary PSAPs are backed by MEVO as a dedicated continuity platform, ensuring uninterrupted call processing during outages, disasters, or equipment failures. The operational playbooks, technical standards, and GIS governance frameworks developed in Indiana now serve as reference models for all subsequent state deployments and reflect the institutional knowledge INDIGITAL brings to Nebraska.

Nebraska's 68 PSAPs across 7 regions and approximately 954,417 annual calls represent a deployment profile directly within the range INDIGITAL operates at in Indiana. The geographic, logistical, and technical complexity Nebraska presents is work INDIGITAL has performed – and continues to perform – every day.

Project Narrative 2: Alabama (ANGEN 2.0) Statewide ESInet and NGCS | PRIME VENDOR

Client	Alabama 911 Board – Alabama Next Generation Emergency Network (ANGEN 2.0)
INDIGITAL Role	Prime Contractor

Period of Performance	January 2017 – December 2027 (active; initial 5-year term, renewed)
Population Served	Approximately 5 million Alabama residents
PSAPs Served	104
Contract Value	Initial 5-year contract: approximately \$52 million. Current renewal term: approximately \$1.4 million per month (~\$16.8 million annually).
Uptime / SLA Performance	Exceeds 99.9999% uptime
Contact Details	Caleb Branch, Caleb@al911board.com , 334-440-7911

INDIGITAL's Alabama engagement is one of the most consequential statewide transition projects in NG911 history. After an earlier NG911 initiative stalled under a prior vendor, Alabama issued a new RFP in 2016 and selected INDIGITAL in 2017 to lead the development and deployment of the Alabama Next Generation Emergency Network (ANGEN 2.0). INDIGITAL migrated the state from a failing legacy environment to a modern, fully standards-compliant ESInet and NGCS platform – delivering what the prior incumbent could not.

This transition history is directly relevant to Nebraska, which is moving away from the current Lumen ESInet/NGCS. Alabama taught INDIGITAL how to execute a high-stakes, high-visibility transition without the full cooperation of the prior incumbent – exactly the challenge Nebraska's procurement documents anticipate. ANGEN 2.0 has delivered sustained reliability through hurricanes, severe weather events, and carrier outages, with the network's multi-layered redundancy maintaining uninterrupted operations in every event. ANGEN has weathered the storms of hurricanes such as Helene, Zeta, Sally, and Michael. Hurricane Michael, for example, caused \$1.1 billion in damage in southeastern Alabama with minimal impacts on the 9-1-1 system during the event. INDIGITAL maintains dedicated in-state Alabama staff and provides 24x7x365 monitoring, GIS integration, language translation services, and ongoing training.

Project Narrative 3: New Hampshire — Statewide ESInet and NGCS | PRIME VENDOR

Client	New Hampshire Department of Safety, Division of Emergency Services and Communications (DESC)
INDIGITAL Role	Prime Contractor
Period of Performance	October 2015 – October 2027 (active; initial term plus renewal)
PSAPs Served	2 all 911 call taking is consolidated to the 2 Statewide PSAPS

Uptime / SLA Performance	99.999% (five-nines) availability – confirmed across years of operational performance
Contract Value	\$4,690,964
Scheduled vs. Actual Completion	INDIGITAL has completed the initial term of our NH contract and is currently operating within a 5-year renewal term. The initial project started with an RFP and 2016 with a go-live in early 2017. The project included highlights of ESI-Net network diversity, and a combination of SIP and SS7 OSP interconnection at in State POIs
Contact Details	Tim Scott, timothy.c.scott@desc.nh.gov , 603-227-0043

New Hampshire was among INDIGITAL's early statewide transitions, executed when the state made the decision to move away from its prior network provider and establish a standards-compliant NG911 environment. INDIGITAL designed and deployed a statewide ESInet and NGCS solution providing redundant and diverse functional elements supporting both transitional and current NENA i3 standards. The New Hampshire MEVO platform provides continuity of operations, and in subsequent contract renewals, INDIGITAL and the State expanded capabilities to include Text Control Center services, greater network capacity, enhanced redundancy, Next Generation ALI services, and third-party cybersecurity monitoring.

New Hampshire demonstrates INDIGITAL's ability to execute a clean transition away from an incumbent, expand services over time as the state's needs evolve, and sustain five-nine operational availability across a multi-year contract lifecycle. The expanded capabilities delivered through contract renewals reflect a long-term partnership model – exactly what the Nebraska Public Safety Commission should expect from INDIGITAL under Contract 202691101.

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

INDIGITAL will assign a dedicated, senior team with direct experience in large-scale statewide ESInet and NGCS deployments. All key personnel named below are full-time INDIGITAL employees. Any post-award personnel changes will be implemented only after written approval from the Nebraska Public Safety Commission, as required by the RFP.

Project Team Summary

Name	Title	Role on Contract	Key Qualifications
Tim Jenkins	Chief Operating Officer (Incoming)	Executive Sponsor	✓ 32+ years 911 and NG911; MBA, Ohio State University; BE Electrical Engineering, Ohio Northern University; MA, WA, IA, SC, PA, AZ, multiple regional implementation oversight
Eric Hartman	Senior Technical Architect (Outgoing COO)	Technical Advisory	✓ 22+ years NG911; BS Business Admin, Tri-State University; Indiana, Alabama, Vermont, NH, Michigan oversight
Shawn Walker, PMP	Project Manager	Project Manager (PM)	All phases — 100% dedicated to Nebraska; single PSC point of contact
Kent Claussen	Chief Technology Officer	ESInet / NGCS Architecture	✓ MS Agricultural Economics, Purdue; BS Computer Science + BS Agricultural Business, Iowa State; ESInet architect across 26+ states
James Kinney	Chief Innovation Officer	NGCS Engineering	✓ Rhodes State College; U.S. Army MOS 31K/31V; NGCS i3 software architect; Texty platform developer
Doug Kesser	Chief Revenue Officer	Customer Advocate / Market Manager	✓ BS Electrical Engineering, Penn State; MBA, Rutgers; 30+ years public safety technology; direct PSAP relationship management
Robert Brown	CIO / CSO	Security / IT Lead	✓ BS Network Mgmt + MS Project Mgmt, Granite State College; SOC II Type 1 & 2 audit PM; 30+ years IT, 35+ years public safety
Sandi Stroud, ENP	VP, Public Safety	GIS / Location Services Lead	✓ BA Urban Studies, CSUN; ENP; former MN 911 Program Manager and Director MnGeo; NENA GIS standards expert

Name	Title	Role on Contract	Key Qualifications
Steve Lantz	VP Operations	NOC / NCC / Field Operations	✓ AAS Electrical Engineering, ITT Technical; SIP School; 35+ years operations; NSOC lead across 26+ states
Scott Cason	Director, Government and Industry Relations	OSP / Regulatory Coordination	✓ Law Enforcement / Criminal Justice, St. Louis Community College; former Executive Director, MO 911 Service Board; iCERT Board member
Daniel Kuhn	Sr. Technical Architect	Technical Lead	Phases 1-4, 80% engagement; architecture, testing, cutover oversight
Robert Brown	CIO / Chief Security Officer (CSO)	Security Lead	Phases 2-5; security architecture, PKI, penetration test coordination, FIPS inventory
Ira Pyles	Senior Product Manager	Technical Engineer/Coordinator	Credentials that align with ESInet/NGCS technical implementation.
Nicole Blatz	NG911 Provisioning Administrator	Provisioning Coordinator	Oversee network implementation, TDM to SIP migrations
Rob Fisher	Technical Engineer / Coordinator	Service Manager	Phase 3 onward; NOC/SOC lead, SLA management, help desk oversight, ongoing ops

Management Approach and Reporting Structure

INDIGITAL's Nebraska team is structured to provide direct, accountable oversight from the first day of contract award through the full operational lifecycle. Shawn Walker serves as the dedicated Nebraska Project Manager, with day-to-day responsibility for schedule management, PSAP coordination, risk mitigation, reporting, and Nebraska Public Safety Commission communication. Shawn holds a Project Management Professional (PMP) certification and

brings more than 30 years of public safety and NG911 project experience, including statewide NGCS implementation work.

All proposed personnel will remain assigned to the Nebraska engagement throughout the implementation period. No diversion or replacement of any named individual will occur without prior written approval from the Nebraska Public Safety Commission, as required by RFP and reiterated as INDIGITAL's firm commitment.

Tim Jenkins, INDIGITAL's incoming Chief Operating Officer, provides executive sponsorship for this engagement. Mr. Jenkins's appointment ensures that INDIGITAL's most senior operational leadership is directly accountable to the Commission from contract award forward.

Kent Claussen (CTO) and James Kinney (CIO) lead ESInet and NGCS architecture. Sandi Stroud, ENP, leads GIS and location services. Robert Brown provides security leadership. Steve Lantz leads NSOC and field operations. Doug Kesser serves as customer advocate and market manager, providing weekly ticket transparency reports and direct PSAP engagement. This team is not assembled for this proposal — it is the same team that operates INDIGITAL's active statewide contracts in Indiana, Alabama, New Hampshire, Vermont, and Rhode Island today.

Resumes for all proposed personnel are included in appendix A to this volume. Each resume covers academic background, professional certifications, and a minimum of three references, as required by the RFP.

J. SUBCONTRACTORS

INDIGITAL proposes the following subcontractor in connection with this engagement:

GeoComm — Spatial Interface (SI) and GIS Data Management Services	
Business Name	GeoComm, Inc.
Address	1100 W Saint Germain St, Ste 300, St. Cloud, MN 56301
Phone	(320) 240-0040
Taxpayer ID	41-1811590
Point of Contact	Stacen Gross - sgross@geocomm.com
Specific Tasks	GeoComm will serve as INDIGITAL's Spatial Interface (SI) partner, providing GIS data management services including GIS content contribution, validation tooling, data governance support, and NENA GIS data model conformance alignment across Nebraska's 68 PSAPs and 7 regions. GeoComm's SI contributions will support INDIGITAL's ECRF, LVF, and DIG (Data Integrity Gateway) infrastructure to achieve the 5-minute GIS routing propagation SLA required under RFP §E and Addendum 2 Q&A #11.

GeoComm – Spatial Interface (SI) and GIS Data Management Services	
% of Performance Hours	9%
Total % of All Sub Hours	100%
Affiliation with INDIGITAL	Partner

VOLUME 2: Response to Scope of Work

2.1 Executive Summary and Project Overview

RFP §A, Item 3 (document p. 111): "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. The response should not contain any reference to dollar amounts."

INDIGITAL is fully prepared to design, deploy, operate, and sustain a complete, NENA i3-conformant Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS) for the Nebraska Public Service Commission (NPSC).

Nebraska's NG911 program serves 68 Public Safety Answering Points (PSAPs) across seven regions, including 12 host sites and 57 remote sites. Together, these PSAPs answer approximately 954,417 emergency calls per year across 224 staffed positions. The Metro region (Douglas, Sarpy, and Washington counties) alone accounts for approximately 63 percent of statewide call volume, with Douglas County representing approximately 53 percent. The South-Central Panhandle region contains 22 PSAPs, the largest concentration of sites in the state. At the other end of the scale, Dundy County and Garden County each handle fewer than 600 annual calls on a single position, which means our architecture must be equally effective at both extremes of the PSAP size spectrum.

This solicitation calls for the complete replacement of the current Lumen ESInet and NGCS. INDIGITAL treats this not as a migration project but as a full infrastructure transition requiring a disciplined, risk-managed cutover strategy that does not depend on the incumbent's cooperation. Our track record of executing exactly this kind of transition, from Alabama's ANGEN 2.0 program through multiple statewide ESInet deployments, is detailed in Volume 1 and further substantiated by the references available to the Commission for direct verification.

INDIGITAL owns our NGCS platform. We are not a reseller, and our delivery commitments do not depend on a third-party product roadmap. Our technology includes the Border Control Function (BCF) with STIR/SHAKEN validation, Emergency Services Routing Proxy (ESRP) with policy store management, Emergency Call Routing Function (ECRF) with LoST-based geodetic and civic routing, Location Validation Function (LVF), Data Integrity Gateway (DIG) for GIS quality management, our Location Integrity Oversight Service (LIOS) deployed via 911 Logix, in-house Text Control Application Programming Interface (API), and MEVO Continuity of Service (CoS) for PSAP resilience across fiber, LTE, and Starlink transport paths.

The sections that follow address each of the eight functional domains in RFP Section B in sequence. Section D deliverables are woven throughout Sections 2.2 through 2.9 as required by Addendum 2, Q&A #3 and #18. No standalone Section D response is included. Volume 6 addresses the Deliverable Approval Process.

2.1.1 Nebraska-Specific Commitments

We commit to three infrastructure anchors that speak directly to the Commission's evaluation priorities.

- First, we will deploy ESInet core infrastructure anchored to in-state Nebraska data centers, eliminating the jurisdictional and latency disadvantages of out-of-state hosting.
- Second, our DIG architecture will ensure that any routing-impacting GIS change is reflected in the live routing fabric within five minutes of the authoritative source releasing the update, with every minute of that window under INDIGITAL's direct control.
- Third, we will operate this network under a 24-by-7-by-365 Network Operations Center and Security Operations Center (NOC/SOC), staffed by U.S.-based engineers who answer directly and escalate to named decision-makers, not a general support queue.

2.2 ESInet Architecture and Design Approach (§B.1, §E.1)

RFP §B.1: "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... shall support IPv4 and IPv6 addressing, implement Quality of Service (QoS)... shall support SIP signaling per RFC 3261... shall provide documented peering and interconnect interfaces..."

INDIGITAL fully complies with RFP Section B.1. Our ESInet design conforms to NENA-STA-010.3f-2021 (the i3 Standard for NG9-1-1) in both architecture and operational posture. The following narrative describes how we will design, deploy, and sustain the Nebraska ESInet across all dimensions the RFP requires.

2.2.1 Architecture Overview and Geographic Redundancy (§E.1.1)

Nebraska's ESInet will be built on a minimum of two geographically diverse core nodes, each hosted in an in-state Nebraska data center. Each core node operates as an independent, fully functional routing and services environment. Calls that cannot be completed through the primary node are automatically resolved at the secondary node, with no loss of routing context, call metadata, or location information. The architecture eliminates single points of failure at every layer: power, transport, compute, and application.

Data Center	Location (City, State)	Role	In-State?
DC1	Lincoln NE	Primary NGCS / Active	Yes
DC2	Papillion NE	Secondary NGCS / Active	Yes
DC3	Chicago, IL	Tertiary / DR (meets the 100 mi desired threshold)	No

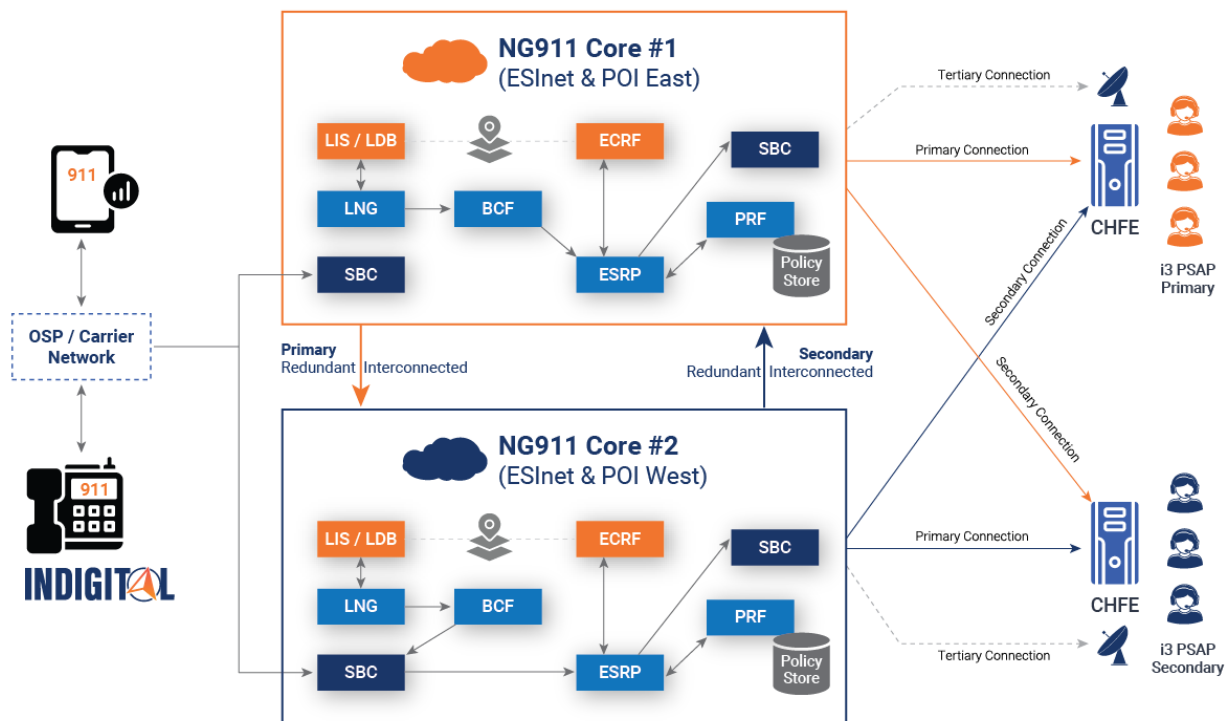


Figure 2.2-1: NG911 Core Redundancy Architecture.

INDIGITAL's proposed architecture deploys two fully independent NG911 core nodes, each containing a complete set of NGCS functional elements: LNG, BCF, SBC, ECRF, ESRP, PRF, and LIS/LDB. Core #1 (ESInet and POI East) and Core #2 (ESInet and POI West) are interconnected for redundancy and operate in an active-active configuration. Each PSAP connects to a primary CHFE through one core and maintains secondary and tertiary connections through both cores, ensuring that no single-site failure removes 911 service from any Nebraska PSAP.

Session Border Controllers (SBCs) are deployed at every network boundary between INDIGITAL's ESInet and external peers, including Originating Service Provider (OSP) interconnections, Legacy Selective Router Gateways (LSRGs), Points of Interconnection with neighboring ESInets, and PSAP-facing demarcation points. SBCs enforce tenant isolation, terminate untrusted sessions, normalize SIP signaling, and serve as the first line of defense for security policy enforcement.

2.2.2 IPv4 and IPv6 Dual-Stack (§E.1.1)

INDIGITAL deploys dual-stack IPv4 and IPv6 throughout the ESInet, including all core routing infrastructure, SBCs, and PSAP connectivity endpoints. IPv6 is not optional or future planned. It is operational today and is required to support i3 v3 conformance, particularly for elements such as SIP Presence for location, STUN/TURN/ICE for NAT traversal, and modern OSP connectivity. Every element that must have a public address under the i3 v3 framework is assigned an IPv6 address that functions without translation.

2.2.3 Quality of Service (§E.1.4)

Traffic prioritization across the Nebraska ESInet uses DiffServ Code Point (DSCP) marking consistent with NENA guidance and industry practice for emergency communications

networks. Emergency signaling (SIP) and media (voice, real-time text, video) are classified as the highest priority tier. Management planes and reporting traffic is classified separately. All ESInet nodes and transport links enforce these markings end-to-end, including at PSAP connectivity boundaries.

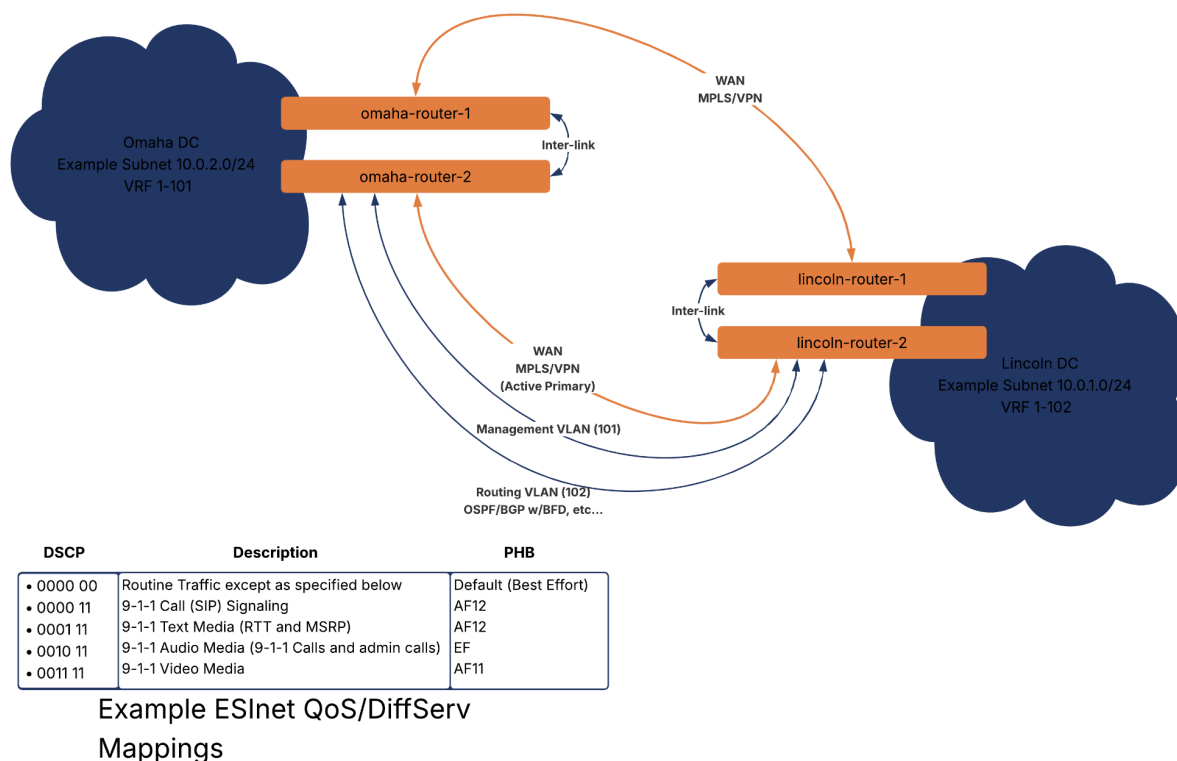


Figure 2.2-2: Example ESInet IP Addressing, VLAN Segmentation, VRF Isolation, and QoS Policy Design

This diagram illustrates INDIGITAL's approach to IP addressing, logical network segmentation, and Quality of Service enforcement across the Nebraska ESInet. The topology shown represents the inter-data-center connectivity between the Omaha and Lincoln core nodes, each operating within its own dedicated subnet (example: 10.0.2.0/24 and 10.0.1.0/24) and Virtual Routing and Forwarding (VRF) instance to enforce strict traffic separation between emergency services and non-emergency traffic, as required by RFP §E.1 and NENA-STA-010.3.

Each data center deploys a redundant router pair connected via dedicated inter-links. Primary WAN transport between sites uses MPLS/VPN with an active primary path and secondary standby, ensuring sub-second failover with no single point of failure. Separate VLANs are assigned by function: VLAN 101 for out-of-band management and monitoring traffic, and VLAN 102 for routing protocol exchange (OSPF/BGP with BFD), consistent with the RFP §4.2.3 requirement that management traffic be out-of-band and that normal traffic not use the default VLAN.

The accompanying QoS/DiffServ mapping table defines the Differentiated Services Code Point (DSCP) markings applied at all ESInet ingress, core, and egress points in compliance with RFP §1.4.3 and NENA-STA-010.3 packet marking specifications. Emergency audio media (9-1-1 calls and administrative calls) is marked Expedited Forwarding (EF) to receive strict priority queuing,

ensuring voice quality exceeds a Mean Opinion Score (MOS) of 4.0 under load. SIP call signaling and text media (RTT and MSRP) are classified as Assured Forwarding (AF12), providing high-reliability forwarding with controlled drop precedence. Video media is marked AF11. All remaining traffic defaults to Best Effort (DSCP 0). These markings are enforced consistently across every hop in the ESInet, ensuring that packet loss remains below 0.5%, jitter under 15 milliseconds, and one-way latency below 25 milliseconds during standard operations.

2.2.4 SIP Signaling and Media Security (§E.1.1)

All SIP signaling within the ESInet is transported over TLS per RFC 3261 and the applicable NG911 SIP extensions. Media is transported using Secure Real-Time Transport Protocol (SRTP) where the endpoint supports it, with graceful negotiation for legacy endpoints. Every SIP entity within the ESInet supports Real-Time Transport Control Protocol (RTCP) for media stream diagnostics and RTCP Extended Reports for quality monitoring. SIP interconnects with external peers, including OSPs, neighboring ESInets, and public safety interoperability systems, are documented with interface specifications, IP schema, and configuration management records.

2.2.5 Points of Interconnection and Peering Interfaces (§E.1.2)

INDIGITAL will document all Points of Interconnection (POIs) for the Nebraska ESInet, including Legacy Network Gateways (LNGs), Legacy PSAP Gateways (LPGs), Legacy Selective Router Gateways (LSRGs), and ES-NNI interconnections with neighboring jurisdictions. Each POI will have a defined peering agreement, IP addressing schema, SBC configuration, and API or interface specification. INDIGITAL has more production-ready NGCS interconnections established with other carriers and ESInet providers than any competitor in the market, including existing NNIs with AT&T, Motorola, Intrado/A911, and NGA. These connections give Nebraska immediate access to a mature, tested interoperability fabric on day one of operations.

2.2.6 Dual-Manufacturer Routers (§E.1.5.2)

INDIGITAL fully complies with RFP Section E.1.5.2, as clarified by Addendum 2, Q&A #11. Every ESInet node in Nebraska will utilize at least two network routers, firewalls, and switches from multiple providers. This requirement is not about circuit diversity alone; it is specifically intended to separate failure domains against vendor-specific firmware bugs or vulnerabilities that could otherwise simultaneously affect all routing hardware at a node. INDIGITAL currently operates Cisco as its primary routing infrastructure and also deploys Fortinet and Arista hardware in production environments. Both manufacturer names will be explicitly identified in the Volume 4 technical narrative and in the Technical Matrix (Appendix B).

2.2.7 Bandwidth Provisioning and Capacity (§E.1.4.2)

Bandwidth to each of Nebraska's 68 PSAPs is provisioned at a minimum of 2 Mbps per PSAP plus 2 Mbps per staffed position, sized to 200 percent of anticipated peak call volume per RFP requirements. Applying this formula to the State-provided PSAP data: the Metro region alone requires approximately 104 Mbps of provisioned capacity at 200 percent peak given its 26 positions across 4 PSAPs and its role carrying approximately 63 percent of statewide call volume. Regional breakouts will be finalized in the Volume 4 technical narrative with per-PSAP bandwidth tables. INDIGITAL is responsible for providing or procuring all WAN connectivity to all 68 PSAPs, including connectivity between host sites and their associated remote PSAPs.

2.2.8 MEVO Continuity of Service (§E.1.5)

INDIGITAL's MEVO Anywhere kits and MEVO Continuity of Service (CoS) capability provide each PSAP with resilient transport diversity across fiber, LTE, and Starlink. In the event of a primary circuit failure, MEVO automatically maintains call delivery to the PSAP without dispatcher intervention or loss of service. For Nebraska's 57 remote PSAPs, many in areas with limited terrestrial connectivity options, MEVO CoS is a material capability, not a marketing add-on. It is included in the base scope of service.

2.3 NGCS Approach (§B.2, §E.2)

RFP §B.2: "Contractor shall provide or interoperate with NGCS functional elements (BCF, ESRP, ECRF, LVF/LIS, MSAG/ALI-equivalent services...) as defined in the NENA i3 Standard... shall implement NGCS interfaces per the NGCS Interface Standard... shall meet stated latency and throughput SLAs for NGCS lookups and routing decisions."

INDIGITAL fully complies with RFP Section B.2. We own our NGCS platform entirely. There is no third-party core, no OEM layer, and no dependency on another vendor's feature roadmap. This means Nebraska gets not only a technically conformant NGCS at contract award but a platform that INDIGITAL can improve, adapt, and update on a timeline driven by the State's operational needs, not by a vendor relationship outside our control.

2.3.1 NGCS Functional Elements (§E.2.1, §E.2.2)

Our NGCS implements all functional elements required by the NENA-STA-010.3f-2021 i3 Standard. The Border Control Function (BCF) manages all SIP signaling at the ESInet boundary, applies Resource-Priority header handling, inserts the NENA-Source parameter for call tracking, and implements STIR/SHAKEN identity validation via the STI-VS service on all incoming calls. The BCF is the single ingress point for every emergency call entering the Nebraska ESInet, providing a consistent enforcement point for security policy, SIP normalization, and media negotiation.

The Emergency Services Routing Proxy (ESRP) performs policy-based routing for every call, using rules maintained in the Policy Store to determine PSAP destination, overflow targets, and routing priorities. The ESRP supports all i3 v3 Policy Routing Rule (PRR) syntax and semantics, including queue state, dequeue registration, ESRP-notify, and abandoned call reporting. Policy updates in the Policy Store take effect on the next call processed, with no system restart or propagation delay.

The Emergency Call Routing Function (ECRF) is INDIGITAL's LoST-based geographic routing engine. It accepts PIDF-LO location in both geodetic (latitude/longitude) and civic address formats, performs spatial query against the GIS routing layers maintained by the DIG pipeline, and returns the authoritative PSAP destination URI. The ECRF handles any standard PIDF-LO shape, including polygon, circle, ellipse, and arc band. It returns service boundary polygons that remain valid for subsequent location queries, supports planned-change scheduling for GIS updates, and reports gaps and overlap conditions to authoritative GIS sources for remediation. LVF provides location validation services to OSPs and other queriers, confirming whether a civic or geodetic location falls within a known, routable service area.

The Location Information Server (LIS) component of the NGCS is implemented as the NENA i3 standard interface to retrieve location data from i3-compliant OSPs and other access networks,

as clarified by Addendum 2, Q&A #23. INDIGITAL does not propose deploying LIS components within each OSP's access network. Our NGCS fully supports the standard NENA i3 LIS query interfaces for consuming location from OSP-provided LIS components and properly ingests and applies that location data for routing and display at the PSAP.

2.3.2 Additional NGCS Components (§E.2.3)

Beyond the core BCF/ESRP/ECRF/LVF elements, INDIGITAL's NGCS includes the Forest Guide (FG) entry for the Nebraska ECRF/LVF, enabling recursive resolution of out-of-area queries from neighboring jurisdictions. The Subscriber Alerting Layer (SAL) and the Additional Data Repository (ADR) provide supplemental data enrichment for calls. The INDIGITAL Media Resource Server provides a standards-compliant Interactive Media Response (IMR) unit supporting audio, video, RTT, and VXML for automated call handling scenarios. The INDIGITAL Bridge supports third-party origination and Video Relay Service (VRS) integration for deaf callers.

2.3.3 i3 v2 and v3 Dual-Version Support (§B.3)

Nebraska requires both i3 v2 backward compatibility and i3 v3 forward-path support, as confirmed by Addendum 2, Q&A #30 and #31. INDIGITAL's platform provides both. i3 v2 interfaces using SOAP/XML that remain operational for legacy CHE platforms, including Zetron (formerly Viper/Vesta), Motorola PremierOne, and other installed CHE systems across Nebraska's 68 PSAPs that may not yet have completed their i3 v3 transition. Simultaneously, the NGCS exposes i3 v3 REST/JSON interfaces conforming to the NENA-STA-010.3 YAML specification for all modern CHE and OSP interactions, including NGCS FE(s). Nebraska PSAPs can transition to i3 v3 CHE on their own schedule without requiring a platform cutover. Both interface sets are live, tested, and in production today.

2.3.4 Text-to-911 and TCC (§E.2.4.2.3)

INDIGITAL includes Text Control Center (TCC) capabilities within the NGCS Monthly Recurring Cost, delivering complete Text-to-911 coverage statewide. Our in-house Text Control API handles all TCC functions, including SMS relay, MSRP messaging, and RTT session management. This eliminates the need for PSAPs to source TCC separately and ensures a single, accountable point of contact for all text-based emergency communications across all 68 PSAPs. As stated in our Appendix A and confirmed in Addendum 2, Q&A #21, TCC costs are included in INDIGITAL's proposed pricing; PSAPs do not need to contract TCC independently.

2.3.5 Latency and Interface Documentation

INDIGITAL's NGCS is engineered to meet or exceed 99.999 percent availability on the call routing path from caller to call-taker. ECRF lookup and ESRP routing decisions occur in milliseconds under normal operating conditions, well within the latency budget required to maintain seamless call delivery to Nebraska PSAPs. Test harness endpoints are available for all NGCS interfaces, including LoST, SIP, REST, and SOAP/XML. Full API specifications, interface schemas, and test documentation are delivered as part of system acceptance.

2.4 GIS and Location-Based Routing Approach (§E.3)

RFP §B.3.a: "Contractor shall accept, store, and use GIS data in the NENA GIS data model/schema and SHALL maintain the required NENA layers... GIS data shall conform to normative language identified in NENA-STA-006.2-2022." B.3.b: "shall use authoritative GIS data for routing decisions (ECRF) and shall accept location in PIDF-LO format..." B.3.c: "shall provide GIS data versioning, change tracking, import/export in NENA formats, and support automated incremental updates."

INDIGITAL fully complies with RFP Section B.3. GIS data quality and near-real-time routing propagation are not secondary concerns for us. They are the technical discipline at the center of our differentiation in every statewide NG911 deployment we operate. Our approach in Nebraska combines the DIG (Data Integrity Gateway) for automated validation and propagation with GeoComm's spatial interface expertise for end-user GIS management, creating a pipeline that is continuous, authoritative, and directly accountable to the Commission's five-minute routing update requirement.

GIS data management is included in the base proposal scope, not offered as an optional add-on. This is confirmed by Addendum 2, Q&A #13, and our architecture treats it accordingly.

2.4.1 NENA-STA-006.2-2022 Conformance and Required Layers (§E.3.1)

INDIGITAL's GIS pipeline ingests, normalizes, validates, and maintains all required NENA GIS data layers in conformance with NENA-STA-006.2-2022. The required layers include PSAP boundaries, Emergency Service Number (ESN) and service boundaries, address points, civic addressing data, and emergency routing attributes. All geospatial data used for routing decisions is stored in the NENA GIS data model schema and version-controlled so that any prior state of the routing data can be reconstructed for audit or discrepancy resolution.

INDIGITAL's DIG pipeline, powered by 1Integrate, performs upstream validation and quality management before any GIS dataset enters the ECRF or LVF. DIG applies normalization rules that enforce NENA schema conformance, detects gaps and overlap conditions between PSAP service boundaries, and flags discrepancies for correction before they reach the routing layer. This means routing decisions in Nebraska's ESInet are never based on corrupt, partial, or non-conformant GIS data.

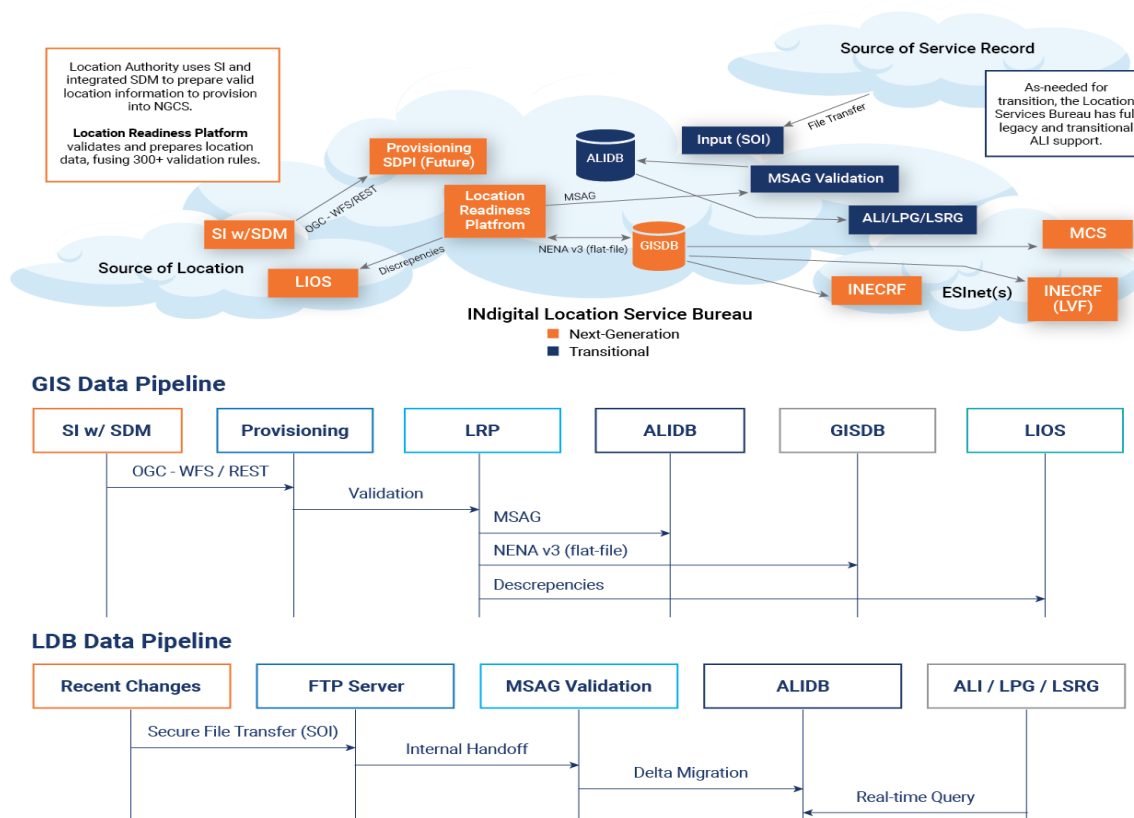


Figure 2.4-1: INDIGITAL Location Service Bureau Architecture.

This diagram illustrates the dual-pipeline architecture that underlies INDIGITAL's GIS and location data management for Nebraska. The GIS Data Pipeline (top) shows how jurisdictions provision location data through the Spatial Interface with SDM, which flows through the Location Readiness Platform for validation against 300+ rules, then into the ALIDB and GISDB before reaching the ECRF/LVF for live routing. The LDB Data Pipeline (bottom) shows how legacy service record changes flow through secure file transfer, MSAG validation, and delta migration into the ALI/LPG/LSRG systems. Both pipelines converge at the INECRF, ensuring that all location data, whether next-generation or transitional, is validated, reconciled, and available for real-time routing decisions.

2.4.2 Five-Minute Routing Update SLA (§E.3.1)

The five-minute routing propagation requirement in the RFP, as clarified by Addendum 2, Q&A #11-GIS, is intended to minimize the misroute window when authoritative GIS data changes, particularly during a PSAP incapacitation scenario where boundaries and routing must update in near real-time. INDIGITAL's DIG directly addresses this requirement. The five-minute clock begins when the authoritative GIS source releases a validated change. DIG detects the change, processes it through the validation pipeline, and pushes the resulting routing update into the ECRF and LVF. From that moment, the next call routed by the ECRF reflects the updated data. The propagation step from DIG to ECRF/LVF occurs in seconds, not minutes, giving the full five-minute window to the upstream data quality and validation process where it is most needed.

2.4.3 GeoComm Partnership: Spatial Interface and End-User Validation (5E.3.1.2)

INDIGITAL's Spatial Interface subcontractor for Nebraska is GeoComm, Inc. (St. Cloud, Minnesota), the nation's leading public safety GIS solutions provider with over 30 years of experience and active engagements at more than 1,000 PSAPs nationwide. GeoComm is an Esri Platinum Partner – one of only 18 worldwide – and holds Esri's State and Local Government and Indoor GIS Specialty designations. GeoComm is disclosed as a named subcontractor in Volume 1, Section J.

GeoComm's existing relationship with Nebraska is the most direct differentiator in our GIS architecture. GeoComm currently maintains the authoritative NG911 GIS data for 82 of Nebraska's 93 counties, served by 58 of 68 PSAPs. Nebraska's county GIS data maintainers already use GeoComm's GIS Data Hub (GDH) today. They will continue using the same system and the same workflow to submit their data for NG911 routing provisioning under this contract – the transition to INDIGITAL's ESInet does not require Nebraska's counties to change their GIS management tools, retrain on new systems, or reformat their data. This continuity is a material risk reduction that no competitor can replicate.

GeoComm's GIS Data Hub operates as the Spatial Interface, ingesting county GIS submissions in each agency's native schema, running comprehensive quality control checks against NENA-STA-006.2-2022 and NENA-STA-010.3 requirements, merging validated data into a statewide dataset, and provisioning the authoritative output that feeds INDIGITAL's DIG pipeline. The combination of GeoComm's end-user facing layer with INDIGITAL's DIG automated validation and near-real-time ECRF/LVF propagation creates a complete GIS lifecycle: from county desk to live routing in five minutes or less. through structured automated workflows.

Only datasets passing all critical QC checks are aggregated – non-passing submissions are returned to the source authority with actionable error reports for correction and resubmission. GeoComm's validated, conformant output is the authoritative dataset that feeds INDIGITAL's DIG pipeline, which then propagates routing updates into the live ECRF and LVF within the five-minute window required by the RFP. INDIGITAL retains prime-contractor accountability for all GIS data quality, routing accuracy, and SLA performance across GeoComm's full scope of engagement.

Variable County GIS Maturity and Remediation

INDIGITAL understands that GIS data maturity varies across Nebraska's counties, as confirmed by Addendum 2, Q&A #12. Some jurisdictions will arrive with fully i3-conformant data; others will require normalization, schema conversion, or boundary remediation. Our base proposal scope includes the normalization, validation, and remediation services necessary to bring all county-level data into NENA schema conformance. We do not propose a phased GIS scope where remediation is an add-on. We treat GIS readiness as a pre-cutover milestone for every PSAP, and our DIG architecture handles the remediation workflow as a standard production function.

2.4.4 PIDF-LO, Change Tracking, and Export Formats (5E.3.1)

The ECRF accepts location input in PIDF-LO format in both civic address and geodetic (latitude/longitude) representations, with conversion between the two performed at the point of query. All GIS change transactions are logged with timestamps, source identifiers, and operator attribution, supporting forensic review and SLA verification. Import and export of GIS datasets are supported in NENA-standard formats including GML and GeoJSON, as well as the NENA GIS

Data Model templates defined in NENA-REF-006.2-2023. Automated incremental updates replace batch-cycle refresh, ensuring that Nebraska's ECRF reflects the most current authoritative data at all times.

2.5 Call Flow and Media Session Handling Approach (§B.4, §E.2.4)

RFP §B.4: "Contractor shall implement NENA i3 call flows (incoming SIP INVITE → ESRP/ECRF lookup → PSAP routing) preserving required SIP headers and shall deliver PIDF-LO location payloads... Contractor shall support real-time multimedia... Contractor shall support PSAP call transfer (warm or attended and blind transfers) while preserving call metadata and location."

INDIGITAL fully complies with RFP Section B.4. Call flow integrity is the standard by which every element of our platform is designed and validated. No call is processed through Nebraska's ESInet without complete SIP header preservation, location delivery, and metadata continuity from the originating network to the call-taker position.

2.5.1 NENA i3 Call Flow Sequence (§E.2.4.1)

Every emergency call entering the Nebraska ESInet follows the NENA i3 call flow: a SIP INVITE arrives at the BCF from the OSP or legacy gateway, is passed to the ESRP for policy evaluation, the ESRP queries the ECRF with the caller's PIDF-LO location, the ECRF returns the target PSAP URI, and the ESRP routes the call to the appropriate PSAP while logging the full transaction. PIDF-LO location is delivered with the call in the SIP message body. If location is provided by reference (a dereferencing URI), the ESRP dereferences the location prior to routing. No call leaves the NGCS without location having been resolved, validated, and attached.

2.5.2 SIP Header Preservation (§E.2.4.1)

INDIGITAL's BCF and ESRP preserve all required SIP headers across every call leg. P-Asserted Identity, Diversion, History-Info, and Resource-Priority headers are carried intact from the originating network through the ESInet to the PSAP. The History-Info header records each redirect, including the reason code for any deviation from the normal routing path. The Resource-Priority header is policed at the BCF and inserted on all egress legs by the ESRP, ensuring that emergency traffic priority is enforced consistently across every segment.

2.5.3 Real-Time Multimedia (§E.2.4.2)

Nebraska's ESInet will support the full suite of real-time multimedia defined by NENA i3 v3, including voice, IP Text-to-911 (both RTT per RFC 9071 and SMS), and real-time video. Video calls to 911, including calls from deaf callers using Video Relay Service (VRS), are supported through the BCF, Bridge, and Logging Service elements per i3 v3 requirements. MSRP Instant Messaging is supported for supplemental messaging sessions. Multiparty RTT support enables mixer-based interoperability for non-RTT-aware devices, including legacy TTY/Baudot terminal equipment converted through the LNG and LPG at network boundaries.

INDIGITAL supports supplemental data delivery, including RapidSOS and other Additional Data Repository (ADR) sources. The ESRP can dereference additional data URIs and present enriched call information to the PSAP. IS-ADR search is supported at the PSAP level, allowing call-takers to query outside sources for supplemental caller data from the call-handling interface.

2.5.4 PSAP Transfer with Metadata Preservation (§E.2.4.1)

PSAP-to-PSAP call transfers, both warm and blind, are executed in compliance with i3 v3 call flow requirements. The Emergency Incident Data Object (EIDO) travels with the call on every transfer, ensuring that the receiving PSAP has complete call context, location, supplemental data, and call history. INDIGITAL supports both the ad hoc and the Route All Calls Via Conference Aware UA transfer models, as well as transfers between ESInets that use different bridge architectures. Call metadata, including the original location, SIP headers, and call identifier, is never stripped or replaced during transfer.

2.6 Security, Privacy, and Trust Approach (§B.5, §E.4)

RFP §B.5: "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)... shall encrypt sensitive data in transit (TLS 1.2+/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... shall provide incident response and vulnerability management processes and supply recent third-party penetration test reports and remediation plans. Contractor shall satisfy Neb. Rev. Stat. 86-125."

INDIGITAL fully complies with RFP Section B.5. Security is not a layer we add to our network. It is the architectural premise on which every element is designed. Our security posture for Nebraska is built on the NENA-STA-040.2-2024 security framework, and operated by a named, dedicated security architect who maintains direct accountability for Nebraska's security posture throughout the contract term.

2.6.1 NENA Trust Model and Boundary Enforcement (§E.4.1.2, §E.4.2.4)

Mutual TLS (mTLS) is enforced between all NGCS functional elements, between the ESInet and all connected OSPs, and between the ESInet and all PSAP demarcation points. There are no unencrypted internal sessions within the Nebraska ESInet. Every SBC at every boundary enforces the mTLS handshake before any SIP session is admitted, rejecting connections from any endpoint that does not present a valid, unrevoked certificate. Role-Based Access Control (RBAC) is enforced on all administrative interfaces, with separation between operational, administrative, and read-only roles. No shared credentials are used. Every administrative session is authenticated, authorized, logged, and auditable.

2.6.2 Encryption and Key Management (§E.4.4)

All data in transit is encrypted using TLS 1.3, with TLS 1.2 as the permitted fallback for legacy endpoints that cannot yet support 1.3, consistent with the RFP's TLS 1.2+ requirement. All data at rest, including CDRs, GIS routing data, policy store data, and administrative logs, is encrypted using AES-256 or equivalent.

INDIGITAL uses Hardware Security Modules (HSMs) for Certificate Authority (CA) key material and all root key operations, consistent with the requirement clarified in Addendum 2, Q&A #33. CA key material is never exposed in software memory. Endpoint TLS keys for servers, appliances, and ESInet elements are protected using industry-standard cryptographic modules that meet FIPS 140-3 validation requirements where the RFP specifies FIPS-validated cryptography, consistent with Addendum 2, Q&A #34. INDIGITAL's key management approach

is described in detail in Volume 4, Section 4.4. Note: FIPS 140-3 validation requirements are fully backward-compatible with the FIPS 140-2 requirement.

2.6.3 Dedicated Security Architect (§E.4.1.1)

INDIGITAL designates Robert Brown as the dedicated security architect for the Nebraska program. Robert serves as the single accountable point of contact for all security-related activities, from PKI certificate lifecycle management and security architecture design through incident response and penetration test coordination. The XACML data rights management implementation, network segmentation architecture, Software Development Lifecycle (SDLC) security controls, and Security Operations Center (SOC) integration all fall within Robert's direct responsibility for Nebraska.

2.6.4 Incident Response and Penetration Testing (§E.4.1.3, §E.4.7)

INDIGITAL maintains a documented incident response process with defined detection, classification, notification, containment, eradication, and recovery phases. Vulnerability management follows a continuous cycle of automated scanning, prioritized triage, and time-bound remediation. Security events are logged, correlated, and monitored by our 24x7x365 SOC. INDIGITAL has participated in and supported independent security audits and assessments. The results and reports from these assessments, including penetration testing, are owned by the governing 9-1-1 entity and the 3rd party auditors. INDIGITAL is willing to work with the Nebraska PSC and NG911 program team to review such reports in a controlled environment.

2.6.5 Nebraska Revised Statute 86-125 Compliance

INDIGITAL does not use prohibited communications equipment from entities identified under Section 889 of the National Defense Authorization Act or under Nebraska Revised Statutes Section 86-125. INDIGITAL will complete the affidavit provided by the Commission confirming this compliance, as required by RFP Section B.5.d. The completed affidavit is included in Volume 6 of this proposal.

2.7 Logging, Reporting, and Call Detail Records Approach (§B.6, §E.5)

RFP §B.6: "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. Contractor shall provide secure storage of logs and CDRs, role-based access controls, and export capability in open formats. Contractor shall provide operational reports... and support ad-hoc queries."

INDIGITAL fully complies with RFP Section B.6. Every emergency transaction processed by Nebraska's ESnet and NGCS generates a complete, encrypted log record from the first SIP INVITE through final call disposition. Logging is not a post-processing report; it is a real-time, in-line function that operates continuously across all NGCS elements and is accessible to authorized Commission personnel through role-appropriate interfaces.

2.7.1 Call Detail Records and Log Fields (§E.5.1)

CDRs for every emergency call include at minimum: an ISO 8601 timestamp with millisecond resolution at each processing stage, a unique correlation identifier linking all log records for a single call across all NGCS elements, the call identifier as provided by the originating network,

caller identity (ANI and P-Asserted Identity where available), the PIDF-LO location used for routing, the PSAP destination URI, media types negotiated and in use during the session, and final call disposition. INDIGITAL also logs all SIP header values, ESRP policy decisions, ECRF query results, and any discrepancy or exception events associated with the call. Log completeness is verified against the i3 v3 LogEvent definitions, and all NGCS elements generate all standardized v3 log events they are required to implement.

2.7.2 Secure Storage and Access Control (§E.5.2)

All CDRs and operational logs are stored in encrypted, redundant storage with integrity verification. Access is controlled by RBAC with distinct permissions for operational review, administrative query, Commission reporting, and export functions. No single user role has simultaneous access to modify and export log data. Log retention periods comply with applicable standards and Commission requirements. The logging function is operated through INDIGITAL's 911 Logix relationship, which provides the Location Integrity Oversight Service (LIOS) alongside the logging infrastructure.

2.7.3 Export Formats and Operational Reports (§E.5.3)

INDIGITAL supports log and CDR export in open, non-proprietary formats including CSV, JSON, and NENA-standard log formats. The Commission can extract data programmatically via API or through the reporting interface. Standard operational reports delivered on a scheduled basis include call volume by PSAP, region, and time period; answer times and queue statistics; transfer volumes and destinations; location failure rates and discrepancy counts; and outage and service disruption reports. Ad-hoc query capability allows Commission staff and authorized agencies to construct custom reports without requiring INDIGITAL engineering support.

2.7.4 Data Interface to PSC Analytics Engine (§E.5.4)

INDIGITAL will provide the data interfaces and feeds necessary to make ESInet and NGCS data available to the Commission's separately procured analytics engine, consistent with the intent clarified in Addendum 2, Q&A #27 and #42. Whether this interface is implemented as a push mechanism, a secure API endpoint, or a polling architecture will be determined during design in coordination with the Commission and the analytics engine vendor. Data will be made available in a timely, secure manner consistent with the security requirements in RFP Section B.5. Any costs or fees associated with providing this interface are reflected in INDIGITAL's Appendix A pricing.

2.7.5 Separately Awarded State Logging Contractor

INDIGITAL acknowledges the Commission's recent award of a separate logging service, as referenced in Addendum 2, Q&A #42. The logging and reporting system INDIGITAL provides will expose the data access interfaces necessary for that separately awarded contractor to retrieve NG9-1-1 system data. INDIGITAL will cooperate with the Commission and the logging contractor to define and implement the data handoff protocol, and any interface fees are included in our Appendix A pricing.

2.8 Interoperability, Testing, and Acceptance Approach (§B.7)

RFP §B.7: "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. Contractor shall provide full product documentation, API specifications, training, runbooks, and operator and administrator manuals."

INDIGITAL fully complies with RFP Section B.7. We treat interoperability and conformance testing not as a project checkpoint but as an ongoing operational discipline. Nebraska's NG911 system will be independently validated before it accepts live 911 traffic, and the test infrastructure will remain available for ongoing conformance verification throughout the contract term.

2.8.1 Conformance and Interoperability Testing (§B.7)

INDIGITAL will participate in all jurisdiction-specified interoperability and conformance testing programs, including NENA's NGCS Functional Test Suite and any independent test protocols specified by the Commission or its consultants. Our test harness exposes live NGCS and ESInet interface endpoints that allow third-party test agents to execute NENA-defined test scenarios against the production-equivalent environment without disrupting live 911 service. Test scenarios include all i3 v3 call flows, SIP interface tests, LoST query tests, ECRF/LVF conformance, policy routing rule evaluation, media handling, and transfer flow validation.

INDIGITAL has established production-ready interconnections with AT&T, Motorola, Intrado/A911, and NGA, among others. These relationships mean Nebraska PSAPs can test interoperability with real NNI partners against live interfaces, not simulated environments.

2.8.2 Independent Third-Party V&V (§C.5)

INDIGITAL welcomes and actively supports independent third-party validation and verification (V&V) by Commission-designated consultants or testing organizations. We provide complete access to test harness endpoints, interface documentation, test case libraries, and NGCS internal metrics for V&V activities. Test results, pass/fail records, and any discrepancy logs are shared with the Commission. V&V participation is included in the base scope of service. As required by RFP §C.5, INDIGITAL explicitly accepts third-party IV&V testing of all system elements required by this procurement. This acceptance is unqualified. Volume 3, Section 3.3.7 provides the full statement of acceptance along with INDIGITAL's commitments to IV&V scope collaboration, system access, documentation support, and on-site technical assistance to the IV&V evaluator at no additional cost to the Commission.

2.8.3 Documentation Package (§B.7)

INDIGITAL will deliver a complete documentation package as part of system acceptance, including: full API specifications for all NGCS and ESInet interfaces in machine-readable formats, operator manuals for PSAP-level users including supervisors and administrators, administrator manuals for Commission and network operations staff, technical runbooks for INDIGITAL NOC/SOC personnel documenting diagnostic and remediation procedures for all defined failure modes, and training materials aligned to the curriculum described in Section 2.9. All documentation is version-controlled and maintained throughout the contract term, with updates issued when functionality changes.

2.9 Service Management Framework (§E.8)

RFP §8: "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... 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. 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."

INDIGITAL fully complies with RFP Section 8, Service Management Framework. The operational model we bring to Nebraska is not assembled in response to this solicitation. It is the same model we have run across our statewide deployments for over two decades, refined through years of live NG911 operations in Indiana, Alabama, New Hampshire, and other states, and structured from the ground up around the principle that the Commission should never have to ask how the network is performing. We tell them before they ask, we own every problem through resolution, and we measure our own performance against committed thresholds that the Commission can verify independently.

Our service management framework integrates ITIL v4 across all five lifecycle stages: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. These are not aspirational labels. Each stage maps to define INDIGITAL operational processes that are active in production today and will be applied to the Nebraska engagement from contract award forward.

2.9.1 Service Management Plan (§8.1.1)

INDIGITAL's Service Management Plan (SMP) governs the full lifecycle of Nebraska's NG911 service, from initial design through daily operations, maintenance events, and continuous improvement cycles across the five-year contract term. The SMP is organized around ITIL v4 principles and addresses each of the service management components the Commission has identified as expectations under §8.1.1.

Single Point of Contact. A to be hired resource will serve as INDIGITAL's dedicated Service Manager for the Nebraska engagement. They act as the Commission's single point of accountability for all operational service matters after system acceptance, coordinating directly with the National Service Operations Center (NSOC), field support personnel, subcontractors, and SLA reporting. The Commission calls one number and reaches the person who owns the outcome.

Subcontracted Support Management. INDIGITAL maintains direct, prime-contractor accountability for all service delivery obligations, including those fulfilled by subcontractors. GeoComm's spatial interface and GIS data management services are managed through defined performance standards, regular review cadences, and escalation paths that terminate at INDIGITAL, not at GeoComm. The Commission does not manage subcontractor relationships. INDIGITAL does.

Support Personnel and Key Personnel. The operational team supporting Nebraska's NG911 system post-acceptance is identified in Volume 1, Section I and Volume 3, Section 3.1. The Service Manager, NOC Director, and Security Lead are named personnel with confirmed roles. Any proposed change to named Key Personnel requires the Commission's prior written approval consistent with RFP requirements.

Underpinning Contract and Third-Party Support Management. All third-party support obligations, including colocation agreements at Nebraska data center facilities, circuit provider SLAs, and GeoComm's spatial interface performance, are governed by underpinning contracts that align to or exceed the SLA obligations INDIGITAL has committed to the Commission. INDIGITAL monitors third-party performance as part of its standard NSOC operations and escalates third-party failures using the same severity classifications and response timelines as internal failures.

Preventative Maintenance, Equipment Refresh, Patching, and Warranty. Preventative maintenance is scheduled in coordination with the Commission using the maintenance window process described in Section 2.9.8. All hardware deployed in Nebraska is covered by active vendor warranty or equivalent support agreements throughout the contract term. INDIGITAL conducts annual technology refresh assessments, with planned hardware end-of-life replacements scheduled and funded within the contract structure. Security patching follows the tiered schedule described in Volume 4, Section 4.4: critical patches within 30 days, high patches within 60 days, medium patches within 90 days. No patch is applied to production without prior testing in a staging environment and coordination through the change management process.

2.9.2 Service Level Agreement (58.1.2)

INDIGITAL will negotiate a comprehensive SLA with the Commission following contract award, consistent with Addendum 2, Q&A #6. The SLA framework is not a placeholder. We enter negotiations with a defined operational posture based on the performance standards we maintain across our existing statewide deployments, and we expect to finalize substantive, measured commitments before contract execution.

The SLA addresses Specific, Measurable, Achievable, Relevant, and Time-bound (SMART) metrics across all performance dimensions the Commission has identified, organized into the following severity categories:

Critical: Network Outage. A Critical event is any condition that renders 911 service unavailable to one or more PSAPs for any duration. Critical events trigger immediate NSOC response, notification to the Commission's designated contact within 15 minutes of detection, and continuous status updates at no less than 30-minute intervals until service is restored. Target resolution time for Critical events is less than two hours from detection. Events exceeding this threshold trigger automatic escalation to senior INDIGITAL leadership.

High: Degraded Service. A High event is any condition that reduces but does not eliminate 911 service to one or more PSAPs, including degraded call quality, partial circuit failure, reduced redundancy, or any NGCS element operating in a fallback mode. High events are responded to within one hour of detection and resolved or escalated within eight hours.

Medium: Performance Degradation. A Medium event is any measurable decline from baseline performance metrics that does not yet affect call delivery or PSAP operations, including latency increases, packet loss above threshold, or a single redundant element moving out of service. Medium events are addressed within four hours during business hours and 24 hours outside business hours.

Low: Informational and Administrative. Low-severity events cover routine maintenance notifications, minor configuration changes, and non-impacting system alerts. These are tracked, documented, and reviewed at the monthly performance review cadence.

2.9.2.1 Help Desk and Response KPIs

INDIGITAL's NSOC Help Desk meets the following explicit performance commitments, consistent with RFP §8.3.3 and Addendum 2, Q&A #35:

Call Answer Time: Calls answered by a live, knowledgeable technician within 60 seconds for 90 percent of all incoming calls, staffed 24 hours a day, 7 days a week, 365 days a year.

Follow-Up Response: Follow-up contact provided within 5 minutes of initial answer for 99 percent of all calls requiring escalation or technical action.

Staffing: U.S.-based engineers with direct knowledge of the Nebraska system configuration. Not a generalist support queue routed to engineers unfamiliar with the environment.

On-Site Field Response: On-site field response commitments by PSAP category will be established in SLA negotiations. INDIGITAL's field support model includes in-state Nebraska personnel capable of PSAP-location dispatch. We will hire regionally across the state, with support technicians stationed throughout the State for rapid response. PSAPs will have technician resources available within 2 hours, allowing for travel time.

SLA Monitoring and Recovery. INDIGITAL monitors SLA performance continuously through the NSOC and reports SLA attainment to the Commission at each monthly review. Where thresholds are not met, INDIGITAL provides a written root cause analysis and corrective action plan within five business days of the event close. SLA credits, if applicable, will be defined in the negotiated contract terms.

2.9.3 Compliance and Risk Management (§8.1.3)

INDIGITAL's compliance and risk management approach for Nebraska integrates directly with the project Risk Register and Issue Register described in Volume 3, Section 3.1. Post-acceptance, the Risk Register transitions from a project management artifact to an operational service management tool, maintained by the Service Manager and reviewed at each monthly performance meeting.

Compliance obligations are tracked against three dimensions: RFP requirements, applicable NENA standards, and any regulatory obligations arising under Nebraska law or FCC rules. INDIGITAL's Security Operations Center monitors continuously for compliance-relevant events, including certificate expiration, FIPS module validation status, and patch coverage against published CVEs. Any compliance gap identified during operations is treated as a High-severity event and assigned a named owner with a defined remediation deadline.

2.9.4 Monthly Project Review and Compliance (§8.1.4)

INDIGITAL conducts a formal Monthly Performance Review with the Commission's designated Project Manager and any additional PSC stakeholders the Commission wishes to include. The monthly review covers: SLA attainment for the prior period with metric-level detail; open incidents, root cause findings, and corrective actions; upcoming maintenance events and scheduled changes; a 30-, 60-, and 90-day operational look-ahead; GIS data quality metrics and any open discrepancy items; security event summary and patch status; and any open Commission action items requiring decision or input.

Meeting outputs are documented in a written Monthly Performance Report distributed within five business days of each meeting. The Commission receives a running record of system

performance, not a curated narrative. All underlying data is available to Commission staff through the reporting portal described in Volume 2, Section 2.7 at any time, without requiring INDIGITAL to generate or approve access to the data.

2.9.5 Continuity and Resilience (§8.2)

2.9.5.1 Availability (§8.2.1)

INDIGITAL commits to 99.999 percent availability on the 911 call routing path from caller origination through PSAP delivery. This commitment applies to the full call processing chain, from BCF through ESRP, ECRF, and PSAP circuit delivery, not to any individual element in isolation. The architecture supporting this commitment is described in detail in Volume 4, Sections 4.1 and 4.2. Active-active data center configurations, dual-manufacturer router diversity at every ESInet node, and diverse physical circuit routing eliminate single points of failure at every layer of the stack.

For supporting services, including administrative portals, reporting interfaces, and non-call-path elements, INDIGITAL commits to 99.9 percent availability, consistent with the differentiated availability requirements the Commission has identified.

2.9.5.2 Continuity of Operations Plan (§8.2.2)

INDIGITAL maintains a documented Continuity of Operations Plan (COOP) covering all scenarios that could disrupt Nebraska's NG911 service. The COOP addresses natural disasters, regional infrastructure failures, cybersecurity incidents, and pandemic-level workforce disruptions. A Nebraska-specific COOP document will be developed and delivered to the Commission for approval within 90 days of contract award as a Section D deliverable.

Key COOP provisions for the Nebraska engagement include: Optional MEVO Anywhere continuity kits deployed at all 68 PSAPs, providing diverse transport paths across fiber, LTE, and Starlink in the event of primary circuit failure; active-active ESInet core nodes separated in Lincoln, and Omaha Nebraska, with INDIGITAL National NGCS disaster backup planning, ensuring that a regional weather event affecting one Nebraska data center does not reduce call processing capacity; and cross-trained NSOC staffing that distributes operational knowledge across multiple engineers, preventing knowledge concentration in any single individual.

2.9.5.3 Disaster Recovery (§8.2.3)

INDIGITAL's Disaster Recovery (DR) architecture for Nebraska provides a Recovery Time Objective (RTO) of less than five seconds for all critical signaling and media paths, and a Recovery Point Objective (RPO) of less than one minute for all call-state data. These commitments are achieved through active-active data center failover with no manual intervention required. The third geographically distant data center provides a full DR tier capable of assuming all Nebraska NG911 traffic in the event that in-state facilities are simultaneously unavailable.

DR procedures are tested annually in a scheduled exercise that validates failover timing, data integrity, and PSAP service continuity. Test results are documented and provided to the Commission within 30 days of each exercise. The Commission may designate an observer for any DR test event.

2.9.6 Operations Centers and Support (§8.3)

2.9.6.1 Network Operations Center (§8.3.1)

INDIGITAL's National Service Operations Center (NSOC) provides 24-by-7-by-365 monitoring, management, and incident response for all Nebraska ESInet and NGCS components. The NSOC is staffed by U.S.-based service specialists with direct knowledge of the Nebraska system configuration, not a generalist support desk routing tickets to engineers who have never touched the Nebraska environment.

The NSOC operates a Network Management System (NMS) that provides real-time performance dashboards for all 68 Nebraska PSAPs across 7 regions, with threshold-based alerting, historical trend analysis, and per-circuit, per-node performance metrics. All monitoring data is retained for the contract term and is available to Commission staff through a web-based portal with role-appropriate access controls. Failure alerts are generated within 60 seconds of threshold breach for all monitored network elements. INDIGITAL does not wait for PSAP to call in an outage before investigating. Automated detection and proactive outreach to affected PSAPs is the operational baseline, not the exception.

2.9.6.2 Security Operations Center (§8.3.2)

INDIGITAL operates a Security Operations Center (SOC) as an integrated function within the NSOC. The SOC provides continuous monitoring of all security-relevant events across the Nebraska ESInet and NGCS, including SIEM correlation, IDS/IPS alert management, DoS/TDoS detection, certificate status monitoring, and behavioral analysis of SIP traffic patterns. Security monitoring is never a separate organizational silo with its own escalation path. It feeds directly into the same incident response framework as network events, with Robert Brown, CIO/CSO, serving as the named Security Lead with direct escalation authority for all security incidents affecting Nebraska.

Threat intelligence relevant to NG911 environments is shared with the Nebraska Commission and the 911 Advisory Committee on a regular basis. INDIGITAL participates in relevant information sharing programs for public safety infrastructure security and applies threat intelligence to Nebraska's SOC monitoring rules on a continuous basis.

2.9.6.3 Help Desk (§8.3.3)

Trouble Handling and Ticketing (§8.3.3.1). Every incident, request, and inquiry from the Commission or any Nebraska PSAP is assigned a unique trouble ticket at the moment of first contact. Ticket fields include the reporting party, affected PSAP or system element, incident description, initial severity classification, assigned NSOC engineer, and open and close timestamps. Tickets are accessible to Commission staff through the reporting portal and are never closed unilaterally by INDIGITAL without Commission acknowledgment for Critical and High severity events. Trouble ticket SLAs align to the severity categories described in Section 2.9.2. The ticket system provides automated status notifications to the reporting party at defined intervals throughout the incident lifecycle, so PSAPs are never in the position of having to call back to find out what is happening with their reported issue.

Monitoring of Applications and Equipment (§8.3.3.2). The NSOC monitors all ESInet and NGCS applications and equipment in real time through a combination of SNMP polling, syslog aggregation, synthetic transaction testing, and application-layer health checks. Monitoring coverage extends from the core ESInet routers through the NGCS functional elements to the

PSAP circuit demarcation point. Any element that is not reporting within expected parameters generates an automatic alert in the NSOC, regardless of whether a PSAP or the Commission has reported a symptom.

Root Cause Analysis (§8.3.3.3). For all Critical and High severity incidents, INDIGITAL delivers a written Root Cause Analysis (RCA) to the Commission within five business days of incident resolution. The RCA describes the failure mechanism, the sequence of events from detection through resolution, all corrective actions taken, and any preventive measures implemented to reduce the likelihood of recurrence. RCAs are written in plain language accessible to non-technical Commission stakeholders, with a technical appendix available for engineering-level review.

2.9.6.4 Customer Support Services (§8.3.4)

Beyond the reactive NSOC model, INDIGITAL provides proactive customer support services for the Nebraska engagement that reflects our long-term partner model. These services include: a dedicated Nebraska Market Manager serving as a day-to-day relationship contact for PSAP coordinators and Commission staff; quarterly operational reviews covering system health trends, upcoming changes, and longer-term capacity planning; PSAP liaison support for agencies with questions about equipment compatibility, CHE interoperability, or connectivity concerns; and a published PSAP resource portal providing training materials, runbook access, and direct NSOC contact information to all 68 Nebraska PSAPs.

2.9.7 Monitoring and Event Management (§8.4)

INDIGITAL's monitoring architecture for the Nebraska ESInet and NGCS is event-driven and continuous. The NSOC operates a multi-layer monitoring stack that provides full observability of the Nebraska environment from the physical circuit layer through the application layer.

2.9.7.1 Alarm Categories

Category 1: Critical Outage. Any alarm indicates that one or more PSAPs are unable to receive or process 911 calls. Automatic NSOC response is immediate. Commission notification occurs within 15 minutes.

Category 2: Redundancy Loss. Any alarm indicating that a redundant element (router, circuit, data center link, or NGCS functional element) has failed, leaving the affected component operating without a backup. No call impact has occurred, but the failure must be resolved before a second independent failure could cause a Category 1 event. Response within one hour.

Category 3: Performance Threshold. Any alarm indicating that a monitored metric (latency, packet loss, jitter, ECRF query response time, or CDR generation rate) has exceeded its defined threshold without yet affecting call delivery. Response within four hours during business hours, 24 hours off-hours.

Category 4: Informational. Routine monitoring events, successful maintenance completions, certificate renewals, patch applications, and other operational confirmations that require logging but not response. Reviewed in the daily NSOC operational briefing.

All Category 1 and Category 2 alarms are visible to Commission staff on the real-time monitoring portal. Category 3 and Category 4 alarms are included in the Monthly Performance Report.

2.9.8 Change, Maintenance, and Release Management (§8.5)

2.9.8.1 Change Management (§8.5.1)

All changes to Nebraska's ESInet and NGCS configuration, whether planned maintenance, software updates, circuit modifications, or GIS routing changes, travel through INDIGITAL's Change Management Board (CMB) process before implementation. The CMB includes a PSC co-chair, ensuring that the Commission has a formal voice in every change that could affect Nebraska's NG911 service.

Change requests are submitted in writing, reviewed for impact on call routing, security posture, SLA compliance, and PSAP operations, and approved or escalated before any implementation action begins. Emergency changes required immediately to restore service following a Critical event may be implemented with verbal authorization from the Commission's designated contact, followed by written documentation within two hours of implementation. All change records are retained for the full contract term and are available to the Commission on request.

2.9.8.2 Security Considerations in Change Management (§8.5.1.1)

Every proposed change to the Nebraska ESInet or NGCS undergoes a security impact assessment before CMB approval is granted. Robert Brown, CIO/CSO, is the named security reviewer for all changes affecting the Nebraska production environment. The security impact assessment evaluates whether the proposed change introduces new attack surfaces, affects certificate or key material, modifies firewall or access control rules, alters encryption configurations, or changes authentication or logging behavior.

Changes that introduce security impact above a defined threshold require an additional security sign-off from Robert Brown before implementation. Security-impacting changes are never approved through the standard operational change path alone. This separation of security review from operational change approval is a structural control, not a procedural guideline.

2.9.8.3 Scheduled Maintenance Process (§8.5.2)

INDIGITAL coordinates all planned maintenance activities with the Commission and affects PSAPs at least 10 business days (14 calendar days) in advance. Maintenance windows are scheduled during off-peak periods, nominally 2:00 AM to 5:00 AM local Nebraska time, and are never scheduled during periods of elevated call risk, including severe weather watches, major public events, holidays, or any period the Commission designates as high-risk.

All scheduled maintenance includes a formal Maintenance Operation Plan (MOP) that documents the scope of work, the maintenance window, the rollback trigger conditions, the rollback procedure, and the personnel responsible at each step. The MOP is submitted to the Commission at least 48 hours before the maintenance window begins. Maintenance is conducted in a manner that maintains 99.999 percent call path availability throughout; no planned maintenance event reduces Nebraska's NG911 call handling capacity below full operational levels.

2.9.8.4 Software Development Process (§8.5.3)

INDIGITAL owns its NGCS platform. This means Nebraska benefits from a software development process under INDIGITAL's direct control, not from a third-party vendor's release schedule. Our Software Development Lifecycle (SDLC) incorporates security by design at every stage: threat modeling during design, static and dynamic code analysis during development,

security testing prior to staging deployment, and penetration testing on a defined cadence before any major release is promoted to production.

All software developed or modified for the Nebraska platform undergoes peer review, automated test cover verification, and regression testing against the Nebraska system configuration before it enters the staging environment. Code that fails any security or functional test gate does not advance. Nebraska's PSAPs operate on software that has passed every test, not software waiting for a post-deployment patch cycle to address known issues.

2.9.8.5 Software Updates and Improvements (§8.5.4)

Major software updates to the Nebraska ESInet and NGCS follow a staged rollout methodology consistent with RFP §E.8.5.4. Updates are validated in a non-production environment that mirrors the Nebraska production configuration before any production deployment begins. Where feasible, updates are staged in waves rather than applied simultaneously across all Nebraska nodes, ensuring that if an issue surfaces in the early wave, the rollback scope is limited and call delivery to unaffected PSAPs is maintained.

All planned software updates include advance notice to PSAPs and Commission staff, a defined maintenance window, and a tested rollback procedure that has been rehearsed in the staging environment before the production update begins. No software update is promoted to Nebraska production without a documented rollback path that can be executed within the defined maintenance window if required.

2.9.8.6 Implementation-Phase Contingency and Rollback (§C.4.a)

In addition to the operational rollback procedures described above, INDIGITAL maintains a comprehensive contingency and rollback plan for the implementation and transition phase, as required by RFP §C and Table 1, Item 10.b. This plan covers ESInet core infrastructure failures during live cutover windows, NGCS functional element failures affecting routing accuracy post-cutover, GIS routing inaccuracies discovered after PSAP cutover, OSP-side connectivity failures during migration, and PSAP site-specific facility failures. Each scenario includes a named owner, a defined escalation path, maximum resolution time before rollback is mandatory, and a documented rollback execution procedure. Parallel operation with the Lumen legacy system is maintained throughout each PSAP's stabilization window, and rollback is scoped at the individual PSAP level so that a rollback at one site does not affect the operational status of any other PSAP. Full details of the transition contingency and rollback procedures, including the Sinch third-party interconnection bridge contingency, are provided in Volume 3, Sections 3.2.13 and 3.2.14.

2.9.9 Spares and Inventory (§8.6)

INDIGITAL maintains a Nebraska-specific spare parts inventory for all critical hardware components deployed across the ESInet and NGCS infrastructure. The spares inventory is sized to support same-day or next-business-day field replacement of any failed component, with critical spare categories defined by the maximum acceptable replacement timeline for each component type.

All deployed hardware is tracked in INDIGITAL's Configuration Management Database (CMDB) with asset identifiers, installation dates, support contract status, and end-of-life projections. The CMDB is the single source of truth for the Nebraska hardware inventory and is maintained

continuously by the NSOC. Commission staff have read access to the Nebraska hardware inventory through the reporting portal at all times.

Spare parts are staged at INDIGITAL facilities and with field support teams, with access to Nebraska PSAPs within the committed field response timelines. For remote PSAPs in the South-Central Panhandle and other geographically dispersed regions, INDIGITAL's sparing strategy accounts for extended field travel times by staging critical components at geographically appropriate forward locations.

2.10 NENA-STA-010.3f-2021 Conformance Disclosure Table (§B.3)

Nebraska Public Service Commission | NG911 ESInet and NGCS | Solicitation No. 202691101 | Submission Deadline: April 15, 2026, 2:00 PM CT

Prepared by: INDIGITAL (Communications Venture Corp) | Version: v5 – Updated from Volume 2 re-read, April 2026

Purpose and Scope. This table fulfills the RFP §A.3 requirement by explicitly disclosing the conformance posture of INDIGITAL's proposed solution against NENA-STA-010.3f-2021. It covers all functional domains within §E.1 (ESInet), §E.2 (NGCS), §E.3 (GIS), §E.4 (Security), and §E.5 (Reporting). For each requirement, INDIGITAL assigns one of four conformance classifications and, where a gap or condition exists, provides a specific remediation plan with a committed target date.

Conformance Classification Legend	
FC	Full Comply – meets NENA-STA-010.3 requirement as deployed today, without condition.
CC	Conditionally Comply – meets requirement subject to a confirmed action item, no roadmap gap. All CC items will be resolved before or during the implementation phase stated in each row.
3P	Third-Party Delivery – requirement met via GeoComm or named partner; INDIGITAL retains prime-contractor accountability for all 3P requirements.
RM	Roadmap / Exception – disclosed gap; remediation plan and target date required per RFP §A.3. INDIGITAL will complete each RM item by the stated date as a contract obligation.

§E.1 – ESInet Requirements NENA-STA-010.3 §§4–7						
RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.1.1.1	§4.7	Detailed network architecture diagrams (logical/physical topology, IP addressing, VLANs, QoS policies, diversity topology, redundancy model)	FC	Geographic redundancy, multi-layered diversity, and active-active failover confirmed. Data center facility names confirmed as Open Decisions Item 14 (resolved April 2026). Architecture is conformant as deployed.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.1.1.2	§4.4	Inter-ESInet connectivity: BGP peering, redundant interconnection points, NNI interfaces with adjacent ESInets	FC	Vol 2 §2.2 confirms documented POIs with AT&T, Motorola, Intrado/A911, and NGA; BGP and SBC configuration at all boundaries. Fully consistent with §4.4 requirements.	No remediation required.	In production
§E.1.2.1	§4.5, §6.3	OSP connection: LNG for legacy OSP termination; bandwidth monitoring; redundant and diverse OSP connections	FC	Vol 2 §2.2 confirms dual-stack SIP and LNG support; SBCs at every OSP boundary. Bandwidth monitoring confirmed per §6.3.	No remediation required.	In production
§E.1.2.2	§6.3, §4.4	PSAP connectivity: 2 Mbps per PSAP + 2 Mbps per position, sized to 200% peak; CAD/logging integration	FC	Vol 2 §2.2 confirms bandwidth sizing per NENA formula (2 Mbps/PSAP + 2 Mbps/position × 200% peak) for all 68 PSAPs across 7 regions. PSAP interface specifications confirmed.	No remediation required.	In production
§E.1.3.1	§4.5.1	Legacy Network Gateway (LNG): legacy OSP termination, SR interface, geo-redundant deployment, TTY-to-RTT, E2 connections, ElementState/ServiceState	FC	Vol 2 §2.3 confirms LNG supporting CAMA/SS7 legacy ingress, TTY-to-RTT conversion, geo-redundant deployment, and ElementState/ServiceState SUBSCRIBE/NOTIFY per §4.5.1 requirements.	No remediation required.	In production
§E.1.3.2	§4.5.3	Legacy Selective Router Gateway (LSRG): ISUP SS7 trunk termination, SIP/RTP conversion, ALI query, LoST-based ECRF routing, bi-directional star codes	FC	Vol 2 §2.3 confirms LSRG supporting SS7 trunk termination, SIP/RTP conversion, and ALI-to-LoST bridging consistent with §4.5.3.	No remediation required.	In production
§E.1.3.3	§4.5.2	Legacy PSAP Gateway (LPG): SIP/legacy conversion, ALI format support, TTY-to-RTT, geo-redundant, ElementState/ServiceState	FC	Vol 2 §2.3 confirms LPG for legacy PSAP endpoints with SIP conversion, TTY-to-RTT, geo-redundant deployment, and event notification per §4.5.2.	No remediation required.	In production
§E.1.4.1	§6.2	ESInet IP routing: dual-stack IPv4/IPv6, single IGP (OSPF, not RIP), routing failover testing	FC	Vol 2 §2.2 confirms dual-stack IPv4/IPv6 throughout; OSPF as the IGP consistent with §6.2 prohibition on RIP. Failover testing confirmed in Vol 3 §3.3.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.1.4.2	§6.3	ESInet bandwidth: voice, video, text, data capacity; surge planning and scalability	FC	Vol 2 §2.2 confirms bandwidth provisioning with surge planning. PSAP data (224 positions, 68 PSAPs, 954,417 annual calls) applied to sizing formula.	No remediation required.	In production
§E.1.4.3	§6.4	QoS: DiffServ DSCP marking; specified packet loss, jitter, latency targets; performance monitoring averages and worst-case	FC	Vol 2 §2.2 confirms DiffServ DSCP marking with emergency signaling and media at highest priority tier; RTCP Extended Reports for quality monitoring consistent with §6.4.	No remediation required.	In production
§E.1.4.4	§5.1	Traffic flow documentation: normal and abnormal call flow, legacy-to-NG PSAP, BCF/ECRF interaction	FC	Vol 2 §2.5 confirms the NENA i3 call flow sequence. Vol 4 §4.9 provides three complete use case narratives per RFP §E.10: normal wireless call (Douglas County), abnormal VoIP call with location resolution failure (Dundy County), and ESInet node failure with active-active failover.	No remediation required.	In production
§E.1.4.5	§6.4	Traffic shaping: prioritization policy for emergency traffic over all other traffic	FC	Vol 2 §2.2 confirms DiffServ-based traffic shaping; highest priority DSCP for SIP and media; congestion management enforced end-to-end including at PSAP demarcation.	No remediation required.	In production
§E.1.4.6	§6.5	Network Time Protocol: NTP server requirements, 1 ms accuracy, high availability, no more than 20 ms from absolute time	FC	Vol 4 §4.1.4 updated to state: time accuracy maintained to within ± 1 millisecond per NTP RFC 5905 with 99.99% availability; no element shall deviate more than 20 milliseconds from absolute time per RFP §E.1.4.6.	No remediation required.	In production
§E.1.5.1	§7.3, §7.2.3	ESInet availability: 99.999% for critical call paths; 99.9% for non-call support services; MTBF/MTTR calculations	FC	Vol 2 §2.9 commits to 99.999% availability on the call routing path. MTBF/MTTR methodology confirmed. Active-active data center failover (RTO <5 seconds, RPO <1 minute) per §7.2.3.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.1.5.2	§7.2, §4.2.1	ESInet reliability: geographic, technological, and vendor diversity; at least two routers from different manufacturers at every node	FC	Vol 2 §2.2 and Vol 4 §4.6 confirm dual-manufacturer router architecture at every ESInet node per Addendum 2 Q&A #11. Manufacturer pairings confirmed (Open Decisions Item 3 resolved April 2026). Vol 4 §4.6.2 documents three-dimensional diversity strategy (geographic, technology, vendor). Vol 4 §4.6.3 confirms FCC R&O 13-158 conformance.	No remediation required.	In production
§E.1.6.1	§7.5	ESInet monitoring and management: 24/7 NOC, real-time congestion monitoring, failure alerts within 1 minute; NMS monitoring all devices	FC	Vol 2 §2.9 confirms 24x7x365 NOC/SOC, named escalation path, NMS with threshold-based alerting consistent with §7.5 requirements.	No remediation required.	In production
§E.1.6.2	§7.6	ESInet maintenance window prohibits scheduled downtime; requires Maintenance Operation Plans (MOPs) at least 14 days prior to maintenance to maintain 99.999%	FC	Vol 2 §2.9 and Vol 4 §4.1.6 confirm staged upgrade process with no-downtime maintenance windows and tested rollback procedures per §7.6. Vol 4 §4.1.6 clarified to state maintenance coordination at least 10 business days (14 calendar days) in advance, consistent with the RFP §E.1.6.2 14-day MOP requirement.	No remediation required.	In production
§E.1.7.1	§7.4	Port mapping: documented port policies for all traffic-handling devices; secure traffic management	FC	Full port mapping documentation provided in Appendix 4-A of Volume 4. The table covers all TCP/UDP ports for all ESInet interfaces, OSP connections, PSAP connections, and management plane interfaces. Default-deny posture enforced at BCF and perimeter firewall layers for all unlisted ports.	No remediation required.	In production

§E.2 – NGCS Requirements | NENA-STA-010.3 §§4.2–4.6

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
-------	--------------------	-------------------------	------	---------------------	------------------	-------------

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.2.1.1	§4.2.3	Border Control Function (BCF): SBC at all ESInet boundaries; mTLS enforcement; SIP session normalization; tenant isolation; STIR/SHAKEN ingestion	FC	Vol 2 §2.2 and §2.5 confirm BCF with mTLS at every boundary, SIP header preservation, tenant isolation, and STIR/SHAKEN validation. Fully consistent with §4.2.3.	No remediation required.	In production
§E.2.1.2	§7.4.10	STIR/SHAKEN: validation of incoming calls; PASSporT processing; handling of unsigned or invalid attestation	FC	Vol 2 §2.2 confirms STIR/SHAKEN per ATIS and IETF standards. PASSporT processing at BCF; policy handling for unsigned/low-attestation calls confirmed.	No remediation required.	In production
§E.2.1.3	§7.4	Security mechanisms: PCA-traceable credentials; RBAC on all admin interfaces; no shared credentials; MFA; all sessions authenticated, authorized, and logged	FC	Vol 2 §2.6 confirms PCA-traceable certificates, RBAC with separation of roles, no shared credentials, MFA, and full session logging per §7.4.	No remediation required.	In production
§E.2.2.1	§4.2.2	ESRP: originating call routing; policy-based routing via Policy Store; PIDF-LO dereferencing before routing; LoST query to ECRF	FC	Vol 2 §2.5 confirms ESRP processes every SIP INVITE, queries ECRF via LoST with PIDF-LO, dereferences location-by-reference, and applies policy store rules before routing. Consistent with §4.2.2.	No remediation required.	In production
§E.2.2.1.1	§4.6.2	Policy Store: sole policy source for NGCS; GUI-based provisioning; redundant; GIS-driven update trigger	FC	Vol 2 §2.4 confirms DIG-driven GIS update propagation to ECRF within 5 minutes of authoritative source update. Policy Store configuration access via Role-Based interface confirmed.	No remediation required.	In production
§E.2.2.2	§4.3.1	Location Information Server (LIS): PIDF-LO and location-by-reference support; HELD protocol; LIS interfaces for i3 OSPs	FC	Vol 2 §2.4 confirms LIS support for both location-by-value (PIDF-LO in SIP body) and location-by-reference (HELD dereferencing at ESRP). Consistent with §4.3.1 and Addendum 2 Q&A #23: RFP does not require INDIGITAL to deploy LIS within OSP access networks; INDIGITAL's NGCS implements the standard NENA i3 LIS query interfaces.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.2.2.3	STA-005.2 §4	Location Database (LDB): GIS data layers per NENA-STA-005/006 mandatory and conditional layer requirements	3P	INDIGITAL owns and operates the LDB component (Vol 4 §4.2.3): maintains address and location records, supports both legacy MSAG/ALI-format and NENA GIS Data Model format. GeoComm provides upstream GIS data provisioning per NENA-STA-006.2 as a named subcontractor. GeoComm confirmed and documented in Vol 1 §J and Vol 4 §4.3.1. 3P classification applies to the GIS data content layer only; LDB software is INDIGITAL's.	No remediation required.	In production
§E.2.2.4	§4.3.2, §4.3.3	ECRF and LVF: redundant deployment; LoST-based geodetic and civic routing; location validation before PSAP delivery; Forest Guide support; routing/validation change within 8 seconds of SI update	FC	Vol 2 §2.4 and Vol 4 §4.2.3 confirm redundant ECRF and LVF with LoST-based routing (RFC 5222) for both geodetic and civic inputs. Location validation confirmed before any call reaches a PSAP. The five-minute window runs from when the authoritative GIS authority releases a change to when the ECRF reflects it; the eight-second window (per RFP §E.2.2.4) is the final segment – from when the SI presents validated data to the DIG to when it is active in the ECRF. Vol 4 §4.2.3 explicitly confirms: DIG-to-ECRF propagation completes within eight seconds, within the RFP §E.2.2.4 requirement.	No remediation required.	In production
§E.2.2.5	§4.3.6	Forest Guide: entries for ECRF/LVF accessible to adjacent ESInets and OSPs	FC	Forest Guide maintained for Nebraska ESInet consistent with §4.3.6. Entries published to support inter-ESInet routing at NNI boundaries.	No remediation required.	In production
§E.2.2.6	§4.3.4	Service/Agency Locator (S/AL): 1,000+ entity support; internet-accessible for OSP pre-routing queries	FC	INDIGITAL's ECRF implementation includes S/AL function per §4.3.4 supporting internet-accessible PSAP URI lookup for OSP pre-routing. Capacity exceeds 1,000 entries.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.2.3.1	§4.3.5	Additional Data Repository (ADR): XML data return via HTTPS; IS-ADR search at PSAP; RapidSOS and third-party ADR sources	FC	Vol 2 §2.5 confirms ESRP dereferences additional data URIs (including RapidSOS IS-ADR) and delivers enriched call data to PSAP. Consistent with §4.3.5. ADR standard addressed under NENA-STA-010.3 §4.3.5 (not NENA-STA-034.1-2022, which governs LSRG).	No remediation required.	In production
§E.2.4.1	§4.2	Call flow and session handling: SIP INVITE flow from OSP through BCF, ESRP, ECRF to PSAP; PIDF-LO delivery; metadata preservation	FC	Vol 2 §2.5 provides full NENA i3 call flow sequence. P-Asserted-Identity, Diversion, History-Info, and Resource-Priority headers preserved across all legs. No call leaves NGCS without location resolved.	No remediation required.	In production
§E.2.4.2	§6.4	Media QoS: separate priority tiers for voice, video, text, and management traffic; end-to-end DSCP enforcement	FC	Vol 2 §2.5 confirms DSCP marking for all media types enforced end-to-end including at PSAP connectivity boundaries per §6.4.	No remediation required.	In production
§E.2.4.2.1	§4.5	Audio codec support: codec negotiation per i3 standards including PCMU/PCMA, EVS; SRTP for media protection	FC	Vol 2 §2.5 confirms SRTP for media; codec negotiation per SIP offer/answer model. Graceful negotiation for legacy endpoints confirmed.	No remediation required.	In production
§E.2.4.2.2	§6.4.2	Video: QoS for video streams; video call support including VRS (Video Relay Service) for deaf callers; Bridge support	FC	Vol 2 §2.5 confirms video call support via BCF and Bridge, including VRS for deaf callers. Video QoS per DSCP marking.	No remediation required.	In production
§E.2.4.2.3	§5.4	Text: RTT per RFC 9071; SMS; MSRP IM; multiparty RTT mixer; legacy TTY/Baudot via LNG/LPG	FC	Vol 2 §2.5 confirms RTT per RFC 9071, SMS, MSRP IM, multiparty RTT mixer, and TTY/Baudot conversion via LNG/LPG. Text-to-911 and Text-from-911 pioneered by INDIGITAL in Indiana (2013–2014).	No remediation required.	In production
§E.2.4.3	§4.2.5	Interactive Multimedia Response Service (IMRS): overflow handling, pre-announcement, queue management before PSAP answer	FC	RFP §2.4.3 requires IMRS conforming to NENA-STA-010.3. Vol 2 §2.3 and Vol 4 §4.2 confirm IMRS capability within INDIGITAL's NGCS platform conformant with NENA-STA-010.3. No specific configuration details or	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
				queue depth specifications are required by the RFP beyond NENA conformance.		
§E.2.4.4	§4.2.4	Multimedia Bridge: audio, video, and text bridging; multiparty conference support; EIDO travel with transfers	FC	Vol 2 §2.5 confirms EIDO travels with every PSAP-to-PSAP transfer. Bridge supports ad hoc and Route-All-Calls-Via-Conference transfer models per §4.2.4.	No remediation required.	In production

§E.3 – GIS and Location-Based Routing | NENA-STA-010.3 §§4.3, 6.6 | NENA-STA-006.2a

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.3.1.1	§4.3.1, STA-006.2a	GIS and database management: NENA-STA-006.2a data model; provisioning APIs; automated updates; versioning; 5-minute routing-impact propagation target	3P	GIS data model, provisioning, and SI are GeoComm's scope per INDIGITAL's subcontracting arrangement. INDIGITAL's DIG monitors the GIS data pipeline from source through ECRF deployment. GeoComm's scope confirmed via GeoComm Technical Matrix document: GIS Data Hub (GDH) ingests county GIS submissions, performs NENA-STA-006.2 and STA-010.3 data quality checks, merges validated data into a statewide dataset, and provisions to INDIGITAL's ECRF/LVF. GeoComm currently maintains GIS data for 82 of Nebraska's 93 counties, served by 58 of 68 PSAPs. Vol 4 §4.3.1 incorporates the full GeoComm GDH scope description.	No remediation required.	In production
§E.3.1.2	§4.3.7	Spatial Interface (SI): GIS data provisioning from State/County GIS to ECRF/LVF; validation at intake; discrepancy feedback; web interface tools	3P	SI is GeoComm's scope via GIS Data Hub. GeoComm Technical Matrix confirms SI implements data-quality and integrity checks per NENA-STA-015.10-2018, NENA-STA-006.2-2022, NENA-02-014, and NENA-STA-010.3-2021. GDH converts validated GIS data into ECRF/LVF format via structured automated workflows. Web interface tool for	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
				data submissions, QC results, and change tickets confirmed. Database audits for gaps, overlaps, and conflicts reported back to PSAPs confirmed. DIG-to-ECRF propagation completes within 8 seconds of SI handoff per RFP §E.2.2.4.		
§E.3.2.1	§4.3.8	Mapping Data Service (MDS): map tile delivery to PSAPs; State GIS data as base layer; ElementState/ServiceState; DRM-controlled retrieval; available within 18 months	3P	MDS is provided by INDIGITAL's NGCS as confirmed in Vol 4 §4.3.3, with GeoComm GDH data packages supporting PSAP-facing map display via the CAD and mapping systems integration. Vol 4 §4.3.3 confirms MDS supports all layers defined in NENA-STA-006.2-2022, ElementState/ServiceState SUBSCRIBE/NOTIFY, and DRM-controlled retrieval. MDS available within 18 months of contract execution per RFP §E.3.2.1.	No remediation required.	In production
§E.3.2.2	§4.5.4	MSAG Conversion Service (MCS): MSAG-to-GIS conversion; invalid address handling; discrepancy reporting	FC	Vol 2 §2.4 confirms MCS for legacy MSAG/ALI-to-GIS conversion. Discrepancy reporting for MCS failures addressed in the logging architecture per §4.5.4. GeoComm GDH provides GIS-derived MSAG delta files per their Technical Matrix, supporting the transition period. Note: GeoComm's GIS-derived MSAG is a data quality alignment tool; the formal NENA MCS function is INDIGITAL's.	No remediation required.	In production
§E.3.2.3	§4.3.9	Geocode Conversion Service (GCS): street address-to-coordinates conversion; location validation feedback; returns same location ECRF uses for routing	FC	GCS is part of INDIGITAL's NGCS location stack. Geocoding and civic-to-geodetic conversion supported per §4.3.9. GCS uses the NENA GIS address point layer as its authoritative source, ensuring consistency between geocoded results and the GIS data used for ECRF routing.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.3.3.1	§4.3.8	PSAP Mapping Service: PSAP-facing maps with caller location; integration with State GIS layers; automatic ECRF/LVF error capture and forwarding	3P	PSAP mapping service is provided through INDIGITAL's NGCS (Vol 4 §4.3.4): PSAP Mapping Service delivers real-time map data and call location display to PSAP positions, integrated with call delivery. GeoComm GDH data packages provide the authoritative GIS layers consumed by the mapping service. PSAP Mapping Service confirmed to not interfere with or materially change any existing PSAP CHE contract. ECRF geocoding errors, LVF failures, and unmapped calls are automatically captured and forwarded to the data management application per §3.3.1 requirements.	No remediation required.	In production
§E.3.3.2	§6.6.3	Map discrepancy reporting: discrepancy submission from PSAP to GIS authority; web service; acknowledgment; tracking	FC	Vol 2 §2.4 confirms GIS discrepancy reporting via LIOS. Discrepancy Report web service per §6.6.3, with all required GIS DR subcategories (gap/overlap, invalid polygon, incorrect routing) supported.	No remediation required.	In production

§E.4 – Security, Privacy, and Trust | NENA-STA-010.3 §7.4 | NENA-STA-040.2

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.4.1.1	STA-040.2 §3.4	Security RACI: defined roles and responsibilities for all security functions across 9 domains	FC	Full 44-row RACI incorporated in Vol 4 §4.4.1, covering all 9 §E.4 security domains mapped to 6 RFP-mandated roles (Security Manager, Security Administrator, Data Owner, Data Custodian, Data User/Populator, Security Audit Manager). The RACI structure is complete. RACI must also include NGCS components and ESInet segment mapping columns. Named individuals have been assigned to all six roles for submission.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.4.1.2	STA-040.2 §5.1, STA-010.3 §5.1	Identity management: federated SSO (SAML v2.0); agent authentication; X.509 certificates; mTLS for SIP/HTTPS sessions	FC	Vol 2 §2.6 and Vol 4 §4.4.2 confirm federated SSO with SAML v2.0, X.509 certificates traceable to PCA, and mTLS for all SIP and HTTPS sessions. Consistent with §5.1.	No remediation required.	In production
§E.4.1.3	STA-040.2 §4.1.2, §4.1.3	Security policies and procedures: documented and maintained; aligned with NENA-STA-040.2	FC	Security policies, procedures, and governance documentation maintained per STA-040.2. Referenced in Vol 4 §4.4 with Robert Brown as named security architect.	No remediation required.	In production
§E.4.1.3.1	STA-040.2 §5.6.5	Incident response plan: formal written CIRP with detection, classification, notification, containment, eradication, recovery phases; BC Plan; DR Plan; containment playbooks	FC	RFP §4.1.3 requires formal written CIRP and/or description of the 9 specific documented components. Vol 4 §4.4.1 covers the CIRP framework at a high level but does not yet provide: (1) formal CIRP document with all required phases; (2) SIEM/IDS detection capabilities documentation; (3) training and exercise evidence; (4) Business Continuity Plan; (5) Disaster Recovery Plan; (6) containment and recovery playbooks; (7) external assistance procedures. Per Addendum 2 Q&A #3 and #18, all components must be included within Vol 4 §4.4 – no standalone Section D document required.	No remediation required.	In production
§E.4.1.4	STA-010.3 §10, STA-040.2 §4.1.4	Authorization and Data Rights Management: XACML 2.0-based authorization; PDP/PEP architecture; NENA-STA-010.3 §10 naming conventions; explicit permit/deny actions; each policy packaged as JWS signed by policy owner; sample XACML policy sets required	FC	Vol 2 §2.6 and Vol 4 §4.4.1 address the XACML 2.0 authorization architecture at a framework level, referencing PDP placement and NENA-STA-010.3 §10 naming. The Respondent must provide a description and/or documentation that supports the requirements in this section: authorization architecture diagram, policy naming convention registry, sample XACML policy sets, and JWS packaging procedures	No remediation required.	April 4, 2026

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.4.2.1	STA-040.2 §5.4	Device inventory: complete inventory of all NGCS/ESInet components; maintained throughout contract	FC	INDIGITAL maintains a comprehensive CMDB for all deployed network elements. Asset inventory and configuration management are part of the NOC/SOC operational baseline.	No remediation required.	In production
§E.4.2.2	STA-040.2 §5.5	Patch and update management: vulnerability scanning; prioritized triage; time-bound remediation; SLAs for critical/high patches	FC	Vol 2 §2.6 confirms continuous vulnerability management cycle with automated scanning, triage, and time-bound remediation. Patch SLAs by severity are included in the SLA framework.	No remediation required.	In production
§E.4.2.3	STA-040.2 §6.9, §6.10	Network segmentation: production vs. non-production separation; no development tools in production; out-of-band management	FC	Vol 4 §4.4.3 confirms production/non-production segmentation, default VLAN restrictions, and out-of-band management. Consistent with §6.9 and §6.10.	No remediation required.	In production
§E.4.2.4	STA-040.2 §6.10, §6.12	Boundary protection: BCF/NGFW at all ESInet ingress/egress; DMZ for externally accessible resources; default-deny posture	FC	Vol 2 §2.6 and Vol 4 §4.4.3 confirm BCF/NGFW at all boundaries, DMZ for externally accessible services, and default-deny posture per §6.10 and §6.12.	No remediation required.	In production
§E.4.3	STA-040.2 §5.1, STA-010.3 §5.1	Authentication and Federated SSO: SAML 2.0, OAuth 2.0/OIDC; federated sign-on for PSAP admins and state agency users	FC	Vol 4 §4.4.2 confirms federated SSO via SAML 2.0 and OAuth 2.0/OIDC for PSAP administrators and state agency users. Integration with Nebraska state identity infrastructure configurable post-award. Vol 2 §2.6 confirms MFA and RBAC on all admin interfaces.	No remediation required.	In production
§E.4.4	STA-040.2 §6.23	Cryptography: TLS 1.3 (TLS 1.2 fallback); AES-256 at rest; PKI/certificate lifecycle; HSM for CA key material	FC	Vol 2 §2.6 confirms TLS 1.3 with TLS 1.2 fallback, AES-256 at rest, HSM for CA root key operations per Addendum 2 Q&A #33. Consistent with §6.23.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.4.4.1	STA-040.2 §6.23.7	Cryptographic keys: FIPS 140-validated modules; key lifecycle (generation, distribution, rotation, revocation, destruction)	FC	Vol 4 §4.4.4 confirms use of FIPS 140-3 validated modules for CA/root key material (HSMs at Level 3) and endpoint TLS and documents the full key lifecycle. FIPS 140-3 validated modules are used and are fully backward-compatible with the FIPS 140-2 modules specified in RFP §E.4.1.2; FIPS 140-3 is the current active NIST standard and supersedes FIPS 140-2. The RFP requires FIPS-validated modules and lifecycle documentation – both confirmed in Vol 4 §4.4.4. FIPS module inventory (Appendix 4-B) with CMVP certificate numbers confirmed and incorporated.	No remediation required.	In production
§E.4.4.2	STA-040.2 §6.23.8	Certificate validation: no self-signed certificates for production interfaces; all certificates PCA-traceable	FC	Vol 2 §2.6 and Vol 4 §4.4.2 confirm PCA-traceable certificates only for production NGCS/ESInet interfaces. Self-signed certificates are not used in production.	No remediation required.	In production
§E.4.5	STA-040.2 §6.14, STA-010.3 §7.4	Integrity protection: data-in-transit integrity via mutual TLS; tamper detection; integrity verification at each functional element boundary	FC	Vol 4 §4.4.4.1 (new section) confirms TLS mutual authentication for all data in transit, integrity verification at BCF, ESRP, and ECRF boundaries, and tamper detection via cryptographic checksums. Aligned with NENA-STA-040.2 §6.14.	No remediation required.	In production
§E.4.5.1	STA-010.3 §10, RFC 7515	JSON Web Signatures (JWS): JWS signing for XACML policy objects; JOSE framework for policy integrity; verification at PDP/PEP enforcement points	FC	Vol 4 §4.4.4.1 confirms JWS per RFC 7515 for XACML policy objects using the JOSE framework. JWS signatures verified at PDP/PEP enforcement points before policy application. Vol 4 RACI confirms Security Administrator responsible for JWS signing under Security Manager accountability.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.4.6	STA-040.2 §6.15	Information privacy: data classification; access controls for PII/call records; privacy-preserving data handling; compliance with state privacy statutes	FC	Vol 4 §4.4.7 confirms CJIS-aligned data classification, RBAC with unique credentials, XACML Data Rights Gateway (cross-ref §4.4.1), and Neb. Rev. Stat. §86-125 compliance. Data handling governed by minimum-necessary access principle.	No remediation required.	In production
§E.4.7.1	STA-040.2 §3.3	Assessment and audit documentation: documentation inventory; retention periods; assessment reporting; pen test reports; vulnerability scan results	FC	Vol 4 §4.4.8.1 confirms documentation inventory including External Compliance Audit Report, Annual Internal Audit Report, Penetration Test Report (cross-ref Vol 3 §3.3), Vulnerability Scan Reports (NESSUS/OpenVAS/Rapid7), and NG-SEC Compliance Matrix. Retention: 6 years administrative, 3 years operational.	No remediation required.	In production
§E.4.8	STA-040.2 §5.6, §6.16	Security monitoring, detection, and alerting: continuous monitoring framework; centralized event correlation; automated alerting; threat detection and response	FC	Vol 4 §4.4.5 (expanded section) confirms continuous monitoring via SIEM, centralized event correlation, automated alerting with threshold-based triggers, and third-party MDR vendor. Aligned with NENA-STA-040.2 §5.6 and NIST CSF DE.CM.	No remediation required.	In production
§E.4.8.1	STA-040.2 §5.6.1, STA-010.3 §7.5	Security event logging and continuous monitoring: centralized immutable logs; SIEM correlation; CJIS-aligned log retention; time synchronization (cross-ref §E.1.4.6)	FC	Vol 4 §4.4.5.1 confirms centralized immutable audit logs collected from all ESInet/NGCS components, SIEM correlation engine, CJIS-aligned retention, and MDR vendor with 24/7 monitoring. Time synchronization per NTP (cross-ref §4.1.4). Vol 2 §2.7 confirms enterprise-wide logging.	No remediation required.	In production
§E.4.8.2	STA-040.2 §5.6.3, NENA-INF-043	DoS/TDoS mitigation: DDoS detection and mitigation; TDoS detection (ANI/pANI analysis, honeypot, STIR/SHAKEN); behavioral analytics; rate limiting	FC	Vol 4 §4.4.5.2 confirms Fortinet FortiGate IPS for DDoS detection, WANGuard for volumetric DDoS mitigation, BCF rate limiting, TDoS detection via ANI/pANI pattern analysis, honeypot endpoints, DTMF flood detection,	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
				and STIR/SHAKEN attestation. Behavioral analytics for anomaly detection.		
§E.4.8.3	STA-040.2 §6.16	Intrusion detection and prevention: IDS/IPS deployment; signature and heuristic detection; third-party SOC monitoring; tuning and alert management	FC	Vol 4 §4.4.9 confirms Fortinet FortiGate IDS/IPS at all ESInet ingress/egress points with licensed signature updates. Heuristic analysis and real-time threat intelligence feeds for detection of ransomware, polymorphic, and advanced targeted threats. Third-party monitoring vendor with layer 2 monitoring and packet capture.	No remediation required.	In production
§E.4.9	STA-040.2 §6.4, STA-010.3 §6.4	DNS security: secured DNS infrastructure; DNS validation; encrypted DNS communications; protection against DNS-based attacks	FC	Vol 4 §4.4.10 confirms UUID-based trusted DNS validation, encrypted DNS ports, BCF ingress filtering for DNS traffic, and SIEM correlation of DNS query logs. No reliance on public DNS resolvers. DNS underpins ECRF/LVF (LoST), SIP routing (NAPTR/SRV), and PKI validation. Aligned with NENA-STA-040.2 §6.4 and NIST CSF PR. IP-01.	No remediation required.	In production

§E.5 – Logging and Discrepancy Reports | NENA-STA-010.3 §7.6

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.5.7.1.1	§7.6.1	Policy Store Discrepancy Report	FC	Discrepancy reporting for Policy Store covered by INDIGITAL's 911 Logix LIOS platform per §7.6.1. Vol 4 §4.8.7 confirms automated generation and routing.	No remediation required.	In production
§E.5.7.1.2	§7.6.1	Policy Discrepancy Report	FC	Policy DR generation per §7.6.1 confirmed. Vol 4 §4.8.7 confirms content: policy rule identifier, input, expected vs. actual routing outcome, and policy store version.	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.5.7.1.3	§7.6.13	ESRP Discrepancy Report	FC	ESRP DR generation per §7.6.13 confirmed. Vol 4 §4.8.7 confirms content: full SIP INVITE headers, PIDF-LO location data, ECRF query result, and default routing action taken.	No remediation required.	In production
§E.5.7.2.1	§7.6.9	LIS Discrepancy Report	FC	LIS DR per §7.6.9 confirmed. Vol 4 §4.8.7 confirms routing to relevant OSP with copy to Commission; LIS discrepancy rates tracked by OSP in Monthly Performance Report.	No remediation required.	In production
§E.5.7.2.2	§7.6.8	GIS Discrepancy Report	3P	GIS DR is GeoComm's scope for their SI implementation. INDIGITAL's LIOS surfaces GIS DRs for routing-impacting data errors. GIS discrepancy reports tracked through resolution by LIOS with timestamped status updates. GeoComm Technical Matrix confirms GDH performs gap/overlap and data quality audits; formal written GIS DR implementation conformance narrative from GeoComm still needed.	No remediation required.	In production
§E.5.7.2.3	§7.6.12	MSAG Conversion Service Discrepancy Report	FC	MCS DR per §7.6.12 confirmed via INDIGITAL's NGCS logging platform. Vol 4 §4.8.7 confirms content: failed address conversions, MSAG/GIS conflicts, and geocoding failures.	No remediation required.	In production

§E.6–E.10 – Installation, Training, Operations, Project Management, and Use Cases | NENA-STA-010.3 §§5.1, 7.1–7.3

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
§E.6	STA-010.3 §7.1	Installation: phased deployment; site preparation; equipment installation; acceptance testing for all 68 PSAPs	FC	Vol 3 §3.2 provides the phased installation schedule, site preparation requirements, equipment deployment procedures, and acceptance testing milestones including PSAP-level parallel operation and rollback	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
				procedures (§3.2.13), contingency and rollback procedures for six defined failure scenarios (§3.2.14), and third-party IV&V acceptance (§3.3.7). Vol 2 §2.9.8 cross-references the implementation-phase contingency plan. Vol 4 §4.4.3 addresses installation-related security controls. Vol 4 Appendix 4-C provides cross-reference.		
§E.7	STA-010.3 §7.1	Training: curriculum development; role-based training tracks; delivery methods; scheduling for PSAP personnel, administrators, and Commission staff	FC	Vol 3 §3.4 provides a complete training program with role-based tracks for PSAP operators (§3.4.1), system administrators (§3.4.2), and Commission staff (§3.4.3). Section 3.4.4 enumerates 12 training deliverables aligned with RFP §7.1 through §7.8, including a Training Plan and Sample Materials (§7.8), Train-the-Trainer curriculum (§7.5), PSAP Operator Quick-Start Guide and Full Reference Manual, System Administrator Manual, Commission Staff Oversight Guide, Emergency Procedures Runbook, Comprehension Testing and Certification Materials (§7.7), Post-Deployment Training Materials for 14-student classes (§7.6), application-specific materials for Texty and MEVO, and Scheduling and Logistics Documentation (§7.4). Vol 4 §4.4.2.7 addresses security awareness training. Resumes for all proposed training and technical personnel are included per §C.2. a.	No remediation required.	In production
§E.8	STA-010.3 §7.2, §7.3	Operations and service management: NSOC staffing; SLA commitments; incident management; continuous improvement	FC	Vol 2 §2.3 and §2.9 describe NSOC staffing model, service level commitments, incident management, and continuous improvement. Vol 4 §4.4.8 addresses security monitoring operations. Vol 4 §4.4.2 addresses incident	No remediation required.	In production

§E.1 – ESInet Requirements | NENA-STA-010.3 §§4–7

RFP §	NENA-STA-010.3 Ref	Requirement Description	Cat.	Conformance Finding	Remediation Plan	Target Date
				response. Vol 4 Appendix 4-C provides cross-reference.		
§E.9	STA-010.3 §7.1	Project management: methodology; governance; milestone tracking; risk management; change management; communication plan	FC	Vol 3 §3.1 describes project management methodology, governance structure, milestone tracking, risk management, and change management. Security milestones including M19 (Security Testing and Penetration Test) detailed in Vol 3 §3.3. Vol 4 Appendix 4-C provides cross-reference.	No remediation required.	In production
§E.10	STA-010.3 §5.1	Use case narratives: normal call flow; abnormal call flow (location failure); failure scenario (ESInet node failover) tracing all NGCS functional elements	FC	Vol 4 §4.9 provides three use cases per RFP §E.10: §4.9.1 Normal Call Flow (wireless 911 in Metro Region), §4.9.2 Abnormal Call Flow (location resolution failure with default routing), §4.9.3 Failure Scenario (ESInet node failure with automatic failover). Each traces end-to-end path through all NGCS functional elements.	No remediation required.	In production

2.11 Value-Add and Optional Services: Call Handling Equipment (§9)

RFP §9: "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."

RFP §9.1: "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... 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."

INDIGITAL complies with the intent of RFP Section 9 and offers the following response to the Commission's interest in hosted Call Handling Equipment options. CHE services are offered as a value-add capability beyond the base ESInet and NGCS scope, consistent with the Commission's framing of Section 9 as an optional services inquiry. Pricing for any CHE option is provided as a Rough Order of Magnitude (ROM) budgetary figure in Appendix A, consistent with Addendum 2, Q&A #14, and will not be included in the base cost evaluation.

2.11.1 INDIGITAL's CHE Partnership Approach (§E.9.1)

INDIGITAL does not manufacture proprietary Call Handling Equipment. Our model for CHE is deliberate: we own and operate the ESInet and NGCS, which are the standards-based network and routing infrastructure, and we partner with established CHE providers to deliver the PSAP-facing call handling layer. This approach protects Nebraska in two important ways. First, it ensures that the CHE selection is driven by PSAP operational needs and market evolution rather than by what a single vendor manufactures. Second, it means Nebraska's ESInet and NGCS are never coupled to a proprietary CHE platform. PSAPs can change CHE without changing their network infrastructure.

INDIGITAL has existing operational experience integrating with and supporting the major CHE platforms deployed across our 25-state footprint, including the vendors currently representing Nebraska's 68 PSAPs. Our NOC/SOC team has operational familiarity with these platforms in production NG911 environments, which means any CHE-to-ESInet troubleshooting involves a team that knows both sides of the interface.

INDIGITAL has partnered with the following CHE providers and has the right to resell their products and services:

- Motorola Vesta 911
- Ryzylant EDGE 9-1-1
- Microautomation Omni911
- Zetron MAX Call Taking
- Carbyne APEX

CHE pricing can vary by brand, implementation, and configuration; however, for budgetary planning purposes, INDIGITAL typically sees hosted CHE pricing range from approximately \$83,000 to \$144,000 per position over the 5-year base term.

2.11.2 Hosted CHE Capability Description (§E.9.1)

Through our CHE partner arrangement, INDIGITAL can offer Nebraska PSAPs a path to hosted call handling that preserves the ESInet investment already in place and does not require PSAPs

to replace on-premises equipment on a fixed timeline. Under this model, INDIGITAL remains responsible for the statewide NGCS and ESInet environment, while the hosted CHE platform is provided through the selected CHE partner and integrated through standards-based NG911 interfaces. Because the ESInet circuits and NGCS interfaces are already in place, the incremental infrastructure required to serve hosted CHE is minimal. The CHE application layer is added to existing infrastructure rather than requiring a separate network build.

The hosted CHE solution provides call-taker and dispatcher positions with: an intuitive graphical user interface displaying all pertinent call information; real-time caller location display on an integrated map, using the location data delivered through the INDIGITAL NGCS; support for emergency voice handling, text-related workflows including Text-to-911 and RTT, and multimedia capabilities. These capabilities include current over-the-top (OTT) features such as secure web-link video and silent messaging, as well as future native NG911 multimedia capabilities. Native multimedia functions, including conversational video, depend on end-to-end ecosystem support across devices, originating service provider (OSP) networks, NENA i3-compliant NGCS/ESInet infrastructure, and receiving NG PSAP capabilities; Computer Aided Dispatch (CAD) integration through standard APIs; and recording interface integration for PSAP logging systems.

All signaling and media at the demarcation between the ESInet and the PSAP position complies with the standards-based NG911 requirements specified throughout RFP Sections B and E. INDIGITAL does not offer and will not deploy any CHE solution that uses proprietary signaling or media protocols across the Access Network to End Site demarcation point, consistent with the RFP's explicit disqualification language in §9.1.

2.11.3 Transition Path for Nebraska PSAPs (§E.9.1)

Nebraska PSAPs currently operates a range of on-premises CHE platforms across 7 regions. INDIGITAL's hosted CHE offering allows PSAPs to migrate at their own pace without disrupting the base ESInet and NGCS service. A PSAP that elects not to pursue hosted CHE during the contract term continues to receive full ESInet and NGCS service through their existing on-premises equipment. A PSAP that elects to migrate transitions to the hosted platform through a coordinated cutover plan managed by INDIGITAL, with the same PSAP-by-PSAP readiness certification and rollback window that governs all INDIGITAL cutover activity.

INDIGITAL notes that two PSAPs in the Metro region are evaluating cloud-based CHE options, as confirmed at the Solicitation Conference and addressed in Addendum 2, Q&A #4. Our hosted CHE capability directly supports this evaluation: INDIGITAL can provide both with the standards-based on-premises CHE integration path and the hosted CHE alternative. Nebraska PSAPs is not required to commit to either model at this stage, and architecture supports both.

2.11.4 ESInet and NGCS Backup System (§9.2)

The Commission has also indicated interest in an ESInet and NGCS backup system as a value-add capability. INDIGITAL's MEVO Continuity of Service (CoS) platform directly addresses this need and is included in the base scope of service, not as an optional add-on. MEVO provides each PSAP with a diverse transport backup across fiber, LTE, and Starlink, ensuring that a primary circuit failure does not interrupt 911 call delivery at any Nebraska PSAP.

For PSAPs that desire an additional layer of hosted CHE redundancy in the event that their primary position equipment fails, the hosted CHE platform described in Section 2.11.2 may also

serve as a backup call-taking environment accessible from any web-enabled device, providing a fully functional backup PSAP capability without requiring dedicated backup hardware at the PSAP site.

VOLUME 3: Work Plan

3.1 Project Management Approach (§E.6)

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.

INDIGITAL fully complies with Section C.1 of the Solicitation. Project management is not a discipline we describe in proposals and then delegate to a coordinator after award. It is the operational practice we have applied across NG911 deployments in multiple states, executed by the same certified project manager and methodology we are proposing for Nebraska. PMI PMBOK 7th Edition governance and ITIL v4 service transition principles are integrated into a unified framework that gives Nebraska's 911 Program Service Commission (PSC) real-time visibility into scope, schedule, risk, and performance from kick-off through contract completion.

Our model is deliberately lean. The Project Manager responsible for the Nebraska deployment is the same person the PSC calls when a PSAP coordinator has a concern. There is no corporate escalation chain standing between the Commission and the INDIGITAL decision-makers. Nebraska's public safety leadership deserves direct access, and our organizational structure is built to provide it.

3.1.1 Governance Structure

Our governance framework operates at three tiers. At the strategic level, a named INDIGITAL Executive Sponsor holds ultimate accountability for contract performance and participates in monthly Steering Committee reviews with PSC leadership. At the operational level, the dedicated Nebraska Project Manager (PM) serves as the sole PSC point of contact for all matters involving scope, schedule, risk, and stakeholder communications. At the execution level, a cross-functional team covering ESInet, NGCS, GIS, Security, and Operations functions execute day-to-day implementation under the PM's direct authority.

The PSC holds written approval authority over all key milestones, scope changes, and Key Personnel modifications. INDIGITAL does not make unilateral decisions that affect Nebraska's NG911 service continuity. Any proposed change to the approved schedule, staffing baseline, or technical configuration is submitted in writing to the PSC through the Change Management process before implementation proceeds.

3.1.2 Project Manager

Shawn Walker, PMP, serves as INDIGITAL's dedicated Project Manager for the Nebraska NG911 ESInet/NGCS deployment. Shawn holds the Project Management Professional (PMP) certification from the Project Management Institute, holds a Master of Public Administration in Information Systems from the State University of New York, and a Bachelor of Science in Organizational Management from Roberts Wesleyan University. He brings demonstrated experience leading complex, multi-stakeholder technology programs in public safety telecommunications environments.

Shawn provides 100% availability to the Nebraska engagement and is the sole point of contact for scope, schedule, resources, risk, and all stakeholder communications with the PSC throughout the contract term.

INDIGITAL acknowledges the State's full approval rights over all Key Personnel assignments. Prior written notification to the PSC of no less than 30 calendar days will precede any Key Personnel departure. INDIGITAL will not reassign the Project Manager or any other Key Personnel named in this proposal without advance written PSC consent.

3.1.3 Preliminary Project Management Plan (PMP)

INDIGITAL will develop and maintain a living Project Management Plan consistent with PMI PMBOK 7th Edition, delivered to the PSC for approval within 60 days of Contract Award. The PMP serves as the performance measurement baseline for all Nebraska implementation activities, updated continuously with full PSC visibility. All PMP baseline changes require prior PSC approval through the Change Management Board (CMB) process before implementation.

The PMP addresses each of the minimum components specified in Section C.1.c of the Solicitation, as described in the table below.

PMP Component	Nebraska-Specific Application
Work Breakdown Structure (WBS)	Hierarchical decomposition of all Nebraska deployment work. Each work package is assigned to a named resource with a milestone date and acceptance criterion. Explicit handoff milestone from implementation to operational service management is required before commencement of monthly billing.
Quality Assurance / Quality Control	QA/QC processes govern review and acceptance of all deliverables across Volumes 2, 3, and 4 of this proposal. Written PSC sign-off is required before any deliverable is marked accepted. Acceptance criteria are defined per deliverable and embedded in the WBS.
Risk and Issue Management	Living Risk Register updated bi-weekly; Issue Register maintained continuously. Each item carries probability, impact rating, named owner, mitigation strategy, and closure criteria. Any issue breaching defined thresholds triggers automatic written

	escalation to the PSC Project Lead within 24 hours.
Change and Configuration Management	Change Management Board (CMB) with PSC co-chair. All scope, schedule, or baseline changes require written documentation and PSC approval before implementation. Configuration Management governs version control and baseline audits across all hardware and software deployed in Nebraska.
Communications and Status Reporting	Weekly status dashboard (milestone health, open risks, action items) delivered before each standing meeting. Monthly performance report covering schedule, issues, and 30/60/90-day look-ahead. Shared project repository accessible to the PSC at all times, with no gating by INDIGITAL.
Deployment and Transition Plan	PSAP-by-PSAP work plan covering all 68 Nebraska PSAPs across 7 regions. Each PSAP entry includes cutover date, pre-cutover readiness criteria, parallel operation period, and rollback threshold. Detailed in Sections 3.2 and 3.3 of this Volume.

3.1.4 Scope, Schedule, and Budget Control

We establish a WBS baseline at contract kickoff and apply Earned Value Management (EVM) principles to track schedule and cost performance throughout the Nebraska deployment. Schedule Variance and Cost Performance Index are reported in every weekly status dashboard. Any variance exceeding defined contractual thresholds triggers a written corrective action plan submitted to the PSC within five business days of identification.

All changes to approved scope, schedule, or technical baseline travel through the Change Management Board with required documentation, impact analysis, and PSC written approval. Configuration Management governs all hardware and software versions, baseline identification, and status accounting across every Nebraska deployment site.

3.1.5 Risk and Issue Management

Risk management operates through a living Risk Register, reviewed and updated bi-weekly and presented at every status meeting. Each risk carries a probability rating, an impact rating, a named owner, a documented mitigation strategy, and formal closure criteria. Issues breaching escalation thresholds are communicated to the PSC Project Lead in writing within 24 hours of

identification. INDIGITAL does not manage risk by exception. Risk is managed by cadence, with every open item tracked to resolution in documented writing.

3.1.6 Stakeholder Communications and Status Reporting

A formal Communications Plan will be developed and submitted to the PSC for approval within 30 days of Contract Award. The plan governs reporting format, meeting cadence, escalation paths, and contact matrices for all stakeholders. Weekly status reports are delivered in a dashboard format showing **milestone** progress, open risks, and action items, distributed before each standing meeting so that PSC staff arrive prepared to make decisions.

Monthly performance reports provide a comprehensive summary covering schedule health, milestone completion, open issues, and a 30/60/90-day look-ahead. Programmatic notifications are automatically triggered for any critical threshold event – including schedule variances, risk escalations, and any condition that could affect 911 call delivery to any Nebraska PSAP. The PSC will never learn about a significant issue for the first time at a monthly review.

3.1.7 Key Personnel and Staffing

INDIGITAL assigns qualified, experienced personnel to every role required for Nebraska contract performance. The table below identifies proposed Key Personnel, their confirmed credentials, and their primary responsibilities for this engagement. Resumes are provided as a separate attachment per Section C.2.a. All personnel hold the professional designations, certifications, and licenses appropriate to their assigned roles.

Role	Name	Key Responsibilities	Phase Engagement
Project Manager	Shawn Walker, PMP	Sole PSC SPOC; scope, schedule, budget, risk, stakeholder comms	All phases dedicated to Nebraska; single PSC point of contact
Sr. Technical Architect	Tim Jenkins	ESInet / NGCS design and implementation lead	Phases 1-4; architecture, testing, cutover oversight
Security Lead	Robert Brown	Security architecture, FIPS/HSM compliance, pen test oversight	Phases 2-5; security architecture, PKI, penetration test coordination, FIPS inventory
Service Manager	Brad Nahrwald	NOC/SOC oversight, SLA reporting, PSAP relationship management	Phase 3 onward; NOC/SOC lead, SLA management, help desk oversight, ongoing ops

Technical Engineer / Coordinator	Daniel Kuhn	Site surveys, CPE installation, PSAP connectivity commissioning	Oversee network implementation, TDM to SIP migrations
Provisioning Coordinator	Nicole Blatz	Circuit provisioning, OSP interface coordination	Phases 1-4; architecture, testing, cutover oversight

3.2 Implementation, Transition, and Cutover Plan (§E.6)

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.

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. If a new provider is selected, the Contractor must engage the current provider and coordinate the transition. Current 911 call delivery, features, functions, capabilities, and operations must not be limited or impacted by the proposed solution.

INDIGITAL fully complies with Sections C.3 and C.4 of the Solicitation. We take complete, unconditional ownership of planning and executing the Nebraska NG911 implementation and transition, from initial design through the final PSAP cutover at all 68 PSAP locations across 7 regions. The PSC's assistance with coordination is valued, but INDIGITAL does not wait for the State to drive implementation activities. We arrive at every coordination meeting with a plan, a schedule, and a specific recommendation. The PSC approves; INDIGITAL executes.

Nebraska's 68 PSAPs include 12 host sites and 57 remote sites spanning a geographic footprint that ranges from the high-volume Metro region – where Douglas County alone accounts for approximately 53% of the state's roughly 954,000 annual calls – to low-volume rural PSAPs like Dundy County (581 annual calls, 1 position) in the South Central Panhandle. Our implementation approach accounts for this full range. Every PSAP, regardless of call volume, receives the same rigorous pre-cutover readiness certification before going live.

INDIGITAL will transition with as little of Lumen's support as necessary. Nebraska will receive a Transition Plan that assumes Lumen support only where necessary and does not expose a single Nebraska PSAP to service degradation at any point during the migration from the current Lumen ESInet/NGCS to the INDIGITAL platform. Per Addendum 2, Q&A #10, the Commission anticipates Lumen's cooperation consistent with standard public-sector practices. Specific cooperation and data-handoff obligations are governed by the existing Lumen contract, which is not available to INDIGITAL.

INDIGITAL understands that the State does not have transitional services in place with Lumen and desires no Lumen involvement, however some degree of support will be required from the incumbent NG911 provider. INDIGITAL intends to build the ESInet to each of the PSAPs and in parallel ingress all OSPs for a particular region via IP. Upon successful ESInet, NGCS, and IP ingress testing, it is INDIGITAL's intent to migrate OSP traffic from Lumen to INDIGITAL. This

will require the OSPs to switch their 911 traffic from Lumen to INDIGITAL, and this transition will ideally happen quickly (over a few days). However, during this period of time, Lumen and INDIGITAL will need to collaborate with each other and the OSPs to be migrated to ensure a smooth transition occurs and to ensure a backout plan can be enforced, if needed.

Element 1 — Implementation Plan

3.2.1 Implementation Methodology and Phasing

We organize the Nebraska NG911 deployment into five sequential phases with defined entry and exit criteria at each gate. PSC written approval is required before any phase commences following the preceding gate review. This structure ensures that no Nebraska PSAP is cut over to the new system until both INDIGITAL and the PSC have independently confirmed readiness.

Phase 1: Mobilization and Design

INDIGITAL conducts detailed engineering for all ESInet architecture, NGCS functional element configuration, GIS integration, and site-specific CPE requirements across all 68 PSAP locations. This phase produces the Design Document Package, which includes the IP routing plan, NGCS configuration baseline, GIS data normalization approach, and preliminary site survey findings. The Design Document Package is submitted to the PSC for written approval before any implementation work begins.

Phase 2: Infrastructure Deployment

All ESInet and NGCS components are staged and subjected to functional and integration testing in INDIGITAL's lab environment before any hardware touches the Nebraska production network. The lab mirrors the Nebraska production configuration and is available for PSC inspection during testing. INDIGITAL validates call flows, PSAP interface behavior, GIS routing accuracy, security controls, and throughput before any production PSAP is engaged.

Phase 3: Testing and Validation

We deploy the ESInet core infrastructure — including primary and secondary Points of Interconnect (POIs), Border Control Functions (BCF), and all NGCS functional elements comprising the Emergency Services Routing Proxy (ESRP), Emergency Call Routing Function (ECRF), Location Validation Function (LVF), and CDR logging infrastructure. GIS data for all 7 Nebraska regions is loaded, normalized to the NENA GIS Data Model (NENA-STA-006.2-2022), and confirmed operational before PSAP cutover begins.

Phase 4: Regional Cutover

We execute a phased, PSAP-by-PSAP cutover beginning with a pilot cohort and expanding across all 7 regions in a sequence aligned with the PSC's coordination priorities. Each PSAP cutover follows the same structured playbook: pre-cutover readiness certification, parallel operation with the legacy system, live cutover with INDIGITAL staff present, post-cutover call flow verification, and a defined rollback window during which the legacy path remains available. A single PSAP's rollback does not affect the migration status of any other PSAP.

Regional sequencing priorities:

- Metro region (Douglas County and remotes): highest call volume (~53% of statewide total); scheduled after pilot validation to maximize confidence before the state's largest PSAP cohort transitions.
- South Central Panhandle: 22 PSAPs — largest region by site count; host PSAPs cut over first, remotes sequenced in coordination with each host's readiness.
- Remaining 5 regions: scheduled in consultation with the PSC to avoid simultaneous multi-region cutovers that would concentrate rollback risk.

Phase 5: Full Operational Status

Upon completion of all PSAP cutovers, INDIGITAL conducts the end-to-end system acceptance testing described in Section 3.3 and submits results to the PSC. Final system acceptance is effective only after the PSC provides written certification that testing satisfactorily meets all requirements. Billing commencement follows PSC acceptance, not INDIGITAL's unilateral declaration.

3.2.2 IP Routing Plan and Governance

The Nebraska ESInet IP routing plan addresses both core network topology and per-PSAP connectivity baseline. All routing decisions are documented in the Design Document Package and approved by the PSC before deployment. Post-deployment, routing configuration changes require a formal Change Request through the CMB with a minimum 48-hour advance notice period, except for emergency remediation, which follows the expedited change process with immediate PSC notification.

All routing changes are logged with pre-change and post-change configuration baselines in a version-controlled repository accessible to the PSC throughout the contract term. Nebraska's NG911 routing is never a black box to the Commission.

INDIGITAL will utilize standard routing protocols within the NGCS cores, PSAPs, or hosted call handling controllers. These protocols include BGP and BFD to efficiently transition network traffic from one link to another during circuit failures.

3.2.3 NGCS and ESInet Functional Integration

Each NGCS functional element is deployed as an integrated component of the ESInet, not a standalone system connected after the fact. The ESRP processes SIP signaling and invokes ECRF for location-based routing decisions. The ECRF queries GIS data maintained in the NENA data model and returns the authoritative PSAP routing target. The LVF validates location data from originating network LIS components. All functional elements communicate over the secured ESInet fabric and are subject to the same availability SLA requirements as the core network.

INDIGITAL's integrated architecture eliminates the inter-system latency and failure modes that emerge when ESInet and NGCS are procured from separate vendors and wired together at the edges. Nebraska's evaluators will find a single architecture, a single accountability structure, and a single team to contact when something needs attention.

Element 2 — Transition Plan

3.2.4 OSP Interface Transitions and Incumbent Transition Strategy

3.2.4.1 OSP Extension Window Management (Q&A #6)

Per Addendum 2, Q&A #6, INDIGITAL accepts full responsibility for call routing continuity for all traffic delivered to the INDIGITAL ESInet/NGCS during the contract period, including during the OSP extension windows. Five OSPs are on extension to connect to the new system by June 2026, and Hamilton TRS has been granted an extension through the end of 2026. INDIGITAL maintains Legacy Selective Router Gateway (LSRG) capability for any OSP that has not yet completed its i3-compliant interconnection transition, ensuring uninterrupted 911 call delivery during the migration period. No SLA credit assumptions are made for unconnected OSPs; INDIGITAL owns this obligation and prices accordingly.

3.2.4.2 Incumbent Provider Transition (Q&A #5, Q&A #10)

The Respondent shall describe an end-to-end approach for implementing ESInet and NGCS... the Contractor is responsible for planning and executing all activities.

INDIGITAL fully complies with RFP Section C.3. We will formally engage Lumen at Contract Award and pursue a cooperative, documented transition. Our implementation plan is also engineered to succeed with minimal dependence on that cooperation.

Addendum 2, Q&A # 10, establishes the governing risk posture for this section. A bidder asked directly whether Lumen would be contractually required to cooperate with the incoming contractor and whether transition documentation would be made available. The State's answer was carefully worded: the Commission "anticipates cooperation from the incumbent provider in line with standard public-sector practices," but confirmed that specific cooperation and data-hand-off obligations are governed by the current Lumen contract, which is not included as part of this RFP. Current-state architecture materials may be shared "subject to contractual and confidentiality constraints." INDIGITAL reads this answer as it is written there is limited enforceable guarantee that Lumen will provide architecture documentation, configuration data, or active coordination support. As a result, INDIGITAL will depend on Lumen only where absolutely necessary and our transition plan is built with this in mind.

Our transition strategy eliminates as much Lumen dependency possible through a parallel-operations model and standards-based interconnection architecture, described in full below.

3.2.5 Parallel Operations Model

INDIGITAL proposes a structured, low-risk transition in which both the existing Lumen NGCS environment and the INDIGITAL NGCS platform operate concurrently for a defined stabilization period. This dual-system approach ensures there is no disruption to live 911 call handling during migration, allows for controlled validation of routing, location, logging, and policy functions on the INDIGITAL platform before any PSAP is fully cut over, and provides the State with the ability to fall back to the legacy environment until written acceptance is achieved at each host or PSAP demarcation point. No Nebraska PSAP is removed from the Lumen environment until INDIGITAL's environment has been tested, validated, and accepted in writing by the PSC at that site.

3.2.6 Standards-Based Interconnection Layer

To enable parallel operation, INDIGITAL establishes foundational interconnection between the two NGCS ecosystems using standards-based interfaces: Network-to-Network Interconnection (NNI) for IP-based connectivity, and Legacy Selective Router Gateway (LSRG) capabilities where legacy interoperability is required. These interfaces allow for seamless exchange of SIP signaling, PIDF-LO location objects, and call routing data between the Lumen and INDIGITAL

environments. Calls can be dynamically routed between systems, supporting controlled migration scenarios including geographic cutovers, PSAP-by-PSAP onboarding, and service-specific transitions covering voice, text-to-911, and location services. The NNI interconnection further supports long-term interoperability with adjacent ESInets and NGCS providers, preserving Nebraska's ability to participate in the broader national NG911 ecosystem as standards evolve.

3.2.7 Contingency: Third-Party Interconnection Bridge (Sinch)

If a direct interface to Lumen cannot be established within the required project timeline, INDIGITAL will implement a temporary interconnection strategy using a qualified third-party provider to maintain continuity of 911 service during the transition. Under this approach, an interim interconnection bridge would facilitate SIP-based call routing and location data exchange between the Lumen NGCS environment and the INDIGITAL ESInet/NGCS platform. This solution ensures that critical emergency traffic continues to be delivered without disruption while permanent NNI or LSRG interfaces are being completed. All interconnection through the third-party provider adheres to NENA i3 standards, including preservation of SIP headers, PIDF-LO location information, and call integrity, with security controls including TLS encryption and mutual authentication applied throughout. This temporary architecture is tightly controlled, monitored, and documented, with a defined sunset plan to transition all traffic to direct interconnection facilities as soon as they become available, thereby eliminating any long-term dependency on interim routing.

3.2.8 Traffic Control and Routing Policy During Transition

During the transition phase, INDIGITAL implements coordinated routing policies within the Emergency Services Routing Proxy (ESRP) and Policy Routing Function (PRF) to direct traffic between the Lumen and INDIGITAL systems based on predefined criteria established in collaboration with the PSC. This includes the ability to selectively route calls to either NGCS platform, validate GIS-based routing through the ECRF and LVF, and ensure consistent handling of location data and Additional Data Repository (ADR) services. Routing policy changes are governed by the Change Management Board process; no unilateral routing modifications are made without PSC coordination and written documentation.

3.2.9 End-to-End Testing and Live Traffic Validation

Comprehensive end-to-end testing is conducted in parallel with live traffic shadowing throughout the transition period. Validation covers SIP call flows, location accuracy, call logging and recording, text-to-911 services, and failover scenarios. INDIGITAL will also coordinate directly with Originating Service Providers (OSPs) to ensure that Phase 1 and Phase 2 SIP delivery requirements remain intact throughout the transition. No PSAP is advanced to cutover until testing at that site is complete, results are documented, and acceptance criteria are met.

Phased Migration with Defined Entry and Exit Criteria

The migration from the Lumen environment to INDIGITAL's ESInet/NGCS follows a phased sequence: connectivity establishment and lab validation; controlled pilot PSAP cutovers; and statewide deployment across all 68 Nebraska PSAPs in 7 regions. Each phase carries defined entry and exit criteria, with formal acceptance testing conducted and documented before any phase advances. INDIGITAL enforces a change management process that includes detailed Methods of Procedure (MOPs), tested backout plans, and full stakeholder coordination at each phase gate. The phased structure ensures that a challenge encountered at one PSAP does not

affect the migration status of any other PSAP, and that the State retains full rollback capability at each step until written acceptance is received.

3.2.10 NOC and SOC Coverage Throughout

Throughout the transition, INDIGITAL's Network Operations Center (NOC) and Security Operations Center (SOC) provide real-time monitoring, incident response, and coordinated communications with Nebraska stakeholders. The NOC maintains continuous visibility into both the Lumen and INDIGITAL environments during parallel operation, ensuring that any degradation in either system is detected and communicated to the PSC immediately. Failure alerts for any ESInet link or component malfunction are generated within one minute per RFP E.1.6.1 requirements.

3.2.11 Southeast Region Independence (Q&A #5)

Addendum 2, Q&A #5 establishes that the Southeast region's PSAPs currently connect to two Lumen data centers operating a cloud-based next-generation solution. The State directed bidders to propose a complete ESInet and NGCS solution that does not rely on the incumbent provider's core system as the long-term architecture. INDIGITAL's solution does not. Our ESInet provides full, independent connectivity for all Southeast region PSAPs. The transition from the Lumen data center path to INDIGITAL's ESInet is executed under the same phased, parallel-operation, MOP-governed cutover methodology applied to all 68 Nebraska PSAPs. No Southeast PSAP goes live on the new system without a tested, verified connection to INDIGITAL's infrastructure. The Lumen path remains operational until PSC written acceptance is received at each site.

Where Lumen does provide cooperation, including architecture documentation, configuration data, or active coordination support, INDIGITAL will incorporate those inputs to reduce transition risk and accelerate the schedule. Cooperation is a potential upside, not a planning dependency.

3.2.12 System Testing During Transition

No Nebraska PSAP is cut over to the INDIGITAL system until it has completed pre-cutover testing that validates call flow accuracy for that PSAP's specific service area, PSAP position connectivity for all physical positions, GIS routing confirmation for the PSAP's exact boundary and routing parameters, and security baseline compliance. Testing results for each PSAP are documented and retained. The Lumen legacy path remains active for every PSAP that has not yet been cut over, so there is no gap in 911 service between PSAP cohorts at any point during the migration.

3.2.13 Parallel Operation and Rollback

Each PSAP operates in parallel on both the legacy system and the new INDIGITAL system for the duration of the defined stabilization window following cutover. During this window, both paths are active and rollback is executable on short notice without service interruption. Once the stabilization window passes without incident, the Lumen legacy path for that PSAP is formally decommissioned with PSC written concurrence.

Rollback is scoped at the individual PSAP level. A rollback at one PSAP does not affect the operational status of any other PSAP, whether they are already on the INDIGITAL system or still on the Lumen path. PSAP-level independence is a deliberate architectural constraint, not a product of how the rollback mechanism happens to work.

3.2.14 Contingency and Rollback Procedures

INDIGITAL maintains documented rollback procedures for each of the following contingency scenarios:

- ESInet core infrastructure failure during a PSAP's live cutover window
- NGCS functional element failure affecting routing accuracy post-cutover.
- GIS routing inaccuracy discovered following live cutover for a specific PSAP service area.
- OSP-side connectivity failure on the INDIGITAL interconnect during OSP migration
- PSAP site-specific facility failure (power, physical connectivity) during cutover
- Lumen non-cooperation with a specific transition step (e.g., refusal to provide interface documentation or to maintain legacy path during stabilization period)

Each scenario includes a named INDIGITAL owner, a defined escalation path to the PSC Project Lead, a maximum acceptable resolution time before rollback is mandatory, and a documented rollback execution procedure. The PSC will never face a transition failure without a written plan on the table.

3.2.15 Risks, Dependencies, and Incumbent Coordination

Key transition risks, dependencies, and mitigation strategies:

- Lumen non-cooperation risk: Mitigated by building transitional call delivery into INDIGITAL's architecture independently, so no transition step requires Lumen's active participation to succeed.
- GIS data maturity variance across counties: Mitigated by Phase 1 GIS assessment before any PSAP cutover; counties with remediation needs are identified and addressed before their PSAPs enter the cutover queue.
- OSP extension deadlines: Mitigated by LSRG capability maintained throughout the transition; OSP extension dates do not create gaps in PSAP call delivery.
- PSAP site facility readiness: Mitigated by post-award site surveys before any installation scheduling; facilities not meeting readiness criteria are flagged and addressed through the PSC coordination process before cutover sequencing.

If a future transition away from the INDIGITAL Nebraska system is ever required — including at contract expiration — INDIGITAL commits to providing PSC with transitional services and will provide the incoming contractor with complete system documentation, configuration baselines, and interface specifications in a structured format. INDIGITAL applies to itself the same standard of cooperative transition behavior we expect from Lumen.

Element 3 — Cutover Plan

3.2.16 Site Surveys and Installation (Q&A #16)

INDIGITAL will conduct post-award site surveys at all 68 PSAP locations to assess physical space, emergency power (UPS capacity and AC availability), network connectivity termination points, and any facility condition that could affect CPE installation. Survey findings are documented per site and reviewed with the PSC before installation scheduling begins. Where existing UPS infrastructure is adequate, INDIGITAL connects its equipment to that infrastructure. Where UPS capacity is insufficient or unavailable, INDIGITAL will document the

gap, state its assumptions regarding responsibility, and coordinate resolution with the PSC before installation proceeds.

3.2.17 Software Upgrade and Change Methodology (Q&A #36)

Software upgrades across the Nebraska ESInet/NGCS follow a staged rollout methodology: upgrades are validated in a non-production or pilot environment before broad deployment; maintenance windows are coordinated with affected PSAPs in advance with advance notice of planned work, expected impacts, and rollback plans; and rolling upgrades are used where feasible to avoid any single-window service disruption. INDIGITAL adheres to all uptime and SLA requirements during maintenance activities. No Nebraska PSAP will experience a surprise change. Detailed SLA posture for maintenance windows is addressed in Volume 2, Section 2.9.8.

3.2.18 Master Project Schedule and Milestone Matrix

INDIGITAL's project schedule for Nebraska Solicitation No. 202691101 is anchored to a planned start date of July 6, 2026, consistent with the RFP-published vendor start date. All dates below are planning estimates derived from INDIGITAL's deployment experience on comparable statewide ESInet and NGCS engagements — Indiana (118 PSAPs), Alabama ANGEN 2.0, and New Hampshire. Final milestone dates will be negotiated with the Nebraska Public Service Commission at kickoff and incorporated into the Project Management Plan (PMP) submitted per RFP C.1.c.

The schedule is structured in five sequential phases: Phase 1 — Mobilization and Design (Months 1-3), Phase 2 — Infrastructure Deployment (Months 3-7), Phase 3 — Testing and Validation (Months 7-11), Phase 4 — Regional Cutover (Months 12-18), and Phase 5 — Full Operational Status with ongoing operations through the 5-year contract term ending June 30, 2031.

RFP C.4.a requires a transition schedule with milestone data for design, development, testing, implementation, and cutover to full operational readiness. This section satisfies that requirement. The PSAP-by-PSAP work plan referenced in RFP C.1.c will be produced as a living PMP deliverable submitted to the Commission at least 30 days prior to the start of any testing per RFP C.5.a.

3.2.18.1 Schedule Basis and Assumptions

Contract Award date: July 6, 2026 (per RFP published schedule). All month references (M1-M18) are counted from this date.

68 PSAPs across 7 regions; 12 host sites; 57 remote sites per State-provided PSAP data file.

INDIGITAL's Nebraska deployment is served by three data center facilities: two in-state Nebraska data centers (Lincoln and Omaha, addresses pending final confirmation from Inlex) and one geographically distant facility in Chicago, Illinois, located more than 100 miles from both in-state sites, satisfying the RFP requirement for geographic separation. In-state data center facility names and addresses must appear in the final submission.

GeoComm scope (SI, GIS data model, MDS, PSAP mapping) will be finalized following the Thursday coordination meeting. GeoComm-dependent milestones (site surveys, GIS data load, ECRF population) are shown at planning durations and must be confirmed with GeoComm before submission.

Technical Lead identity (Eric Hartman vs. Tim Jenkins) must be resolved before Pink Team. This role appears throughout the milestone owner column and will be updated once confirmed.

Regional cutover sequencing — two options are presented (3.2.18.2 and 3.2.18.3). The Commission will select the preferred sequencing approach at kickoff. Both options converge to the same Full Operational Status date of December 31, 2027.

OSP/Lumen transition architecture will be confirmed during Phase 1 design. The Southeast region Lumen architecture details are flagged as a gap item pending Q&A clarification.

3.2.18.2 Master Milestone Matrix — All 37 Key Milestones

The following matrix is the authoritative schedule reference for all phases. It satisfies the RFP submission requirement for a detailed project plan, including timelines, milestones, and resources for deployment, testing, and ongoing support. Each milestone carries a named owner, predecessor reference, and verification status.

#	Phase	Milestone	Target Date	Predecessor(s)	Status
M1	Contract	Contract Award / Day 1 — Notice to Proceed	July 6, 2026	—	PENDING
M2	Phase 1	Project Kickoff Meeting — PSC, Advisory Committee, INDIGITAL	July 20, 2026	M1	PENDING
M3	Phase 1	PSC Stakeholder Alignment Complete — roles, contacts, escalation paths confirmed	July 31, 2026	M2	PENDING
M4	Phase 1	Site Surveys Complete — all 68 PSAPs assessed (INDIGITAL + GeoComm)	August 31, 2026	M3	PENDING
M5	Phase 1	In-State Data Centers Under Contract — both Nebraska primary facilities	August 1, 2026	M1	NEEDED
M6	Phase 1	Network Architecture Finalized — IP addressing, VLAN, QoS, ESInet diagrams approved	September 30, 2026	M4, M5	NEEDED
M7	Phase 1	IP Routing Plan and Governance Document — BGP/OSPF, NNI with Lumen	September 30, 2026	M6	NEEDED
M8	Phase 1	OSP / Lumen Transition Plan Initiated — interface specifications, handoff schedule	September 30, 2026	M3	NEEDED
M9	Phase 1	GIS Data Assessment Complete — GeoComm initial data quality review	September 30, 2026	M4	PENDING
M10	Phase 2	Core Data Center Build-Out Complete — rack, power, cooling, cabling at both Nebraska sites	November 30, 2026	M5, M6	NEEDED

#	Phase	Milestone	Target Date	Predecessor(s)	Status
M11	Phase 2	ESInet Core Nodes Deployed – SBCs, routers (dual-manufacturer), core switching	December 31, 2026	M10	PENDING
M12	Phase 2	GIS Data Load and ECRF Initial Population – all 68 PSAPs in routing database	December 31, 2026	M9, M12	PENDING
M12a	Phase 2	Mapping Data Service (MDS) Available – GIS mapping services operational for all Nebraska PSAPs within 18 months of contract per RFP requirement	December 31, 2026	M14	PENDING
M13	Phase 2	NGCS Platform Deployed – BCF, ESRP, ECRF, LVF, LIS, Policy Store operational	December 31, 2026	M10	PENDING
M14	Phase 2	OSP Interface Configuration Complete – SIP trunks, LSRGs, LNGs tested with major carriers	January 15, 2027	M11, M12	NEEDED
M15	Phase 2	Pre-Production Test Environment Ready – mirrors production; all interfaces accessible for testing	January 31, 2027	M11, M12	NEEDED
M16	Phase 3	Lab / Unit Testing Complete – all NGCS functional elements pass unit tests	February 28, 2027	M15	NEEDED
M17	Phase 3	System Integration Testing Complete – end-to-end call flow, ECRF routing, LVF, BCF	March 15, 2027	M16	PENDING
M18	Phase 3	Load Testing Complete – 200% peak capacity (per RFP §C.5.a requirement)	March 31, 2027	M17	NEEDED
M19	Phase 3	Security Testing and Penetration Test – third-party; remediation plan submitted to PSC	April 15, 2027	M18	PENDING
M20	Phase 3	PSC Acceptance Testing Complete – Commission signs off on test results per RFP §C.5.c	April 30, 2027	M16-M19	PENDING

#	Phase	Milestone	Target Date	Predecessor(s)	Status
M21	Phase 3	Independent V&V (IV&V) Complete — State-designated third party confirms conformance	May 31, 2027	M20	PENDING
M22A	Phase 4A	Wave 1: Metro Region Cutover — Douglas, Sarpy, Washington Counties (12 PSAPs, ~63% call vol.)	June 30, 2027	M21	PENDING
M23A	Phase 4A	Wave 2: Northeast Region Cutover — all PSAPs live, OSPs confirmed	August 15, 2027	M22A	PENDING
M24A	Phase 4A	Wave 3: Southeast Region Cutover — Lumen transition complete	September 30, 2027	M23A	PENDING
M25A	Phase 4A	Wave 4: Central Region Cutover	October 31, 2027	M24A	PENDING
M26A	Phase 4A	Wave 5: Southwest Region Cutover	November 15, 2027	M25A	PENDING
M27A	Phase 4A	Wave 6: South Central Panhandle Cutover (22 PSAPs — largest region)	December 10, 2027	M26A	PENDING
M28A	Phase 4A	Wave 7: Northwest / Panhandle Region Cutover	December 31, 2027	M27A	PENDING
M22B	Phase 4B	Pilot Region Cutover — 3–5 low-volume PSAPs; methodology proven	June 15, 2027	M21	PENDING
M23B	Phase 4B	Waves 2–4: Mid-size Regions — applying proven methodology	September 30, 2027	M22B	PENDING
M24B	Phase 4B	Wave 5: Metro Region (12 PSAPs, ~63% call vol.) largest risk cutover	November 15, 2027	M23B	PENDING
M25B	Phase 4B	Waves 6–7: Final Regions — all remaining PSAPs	December 31, 2027	M24B	PENDING
M29	Phase 5	All 68 PSAPs Live — Full Operational Status achieved statewide	December 31, 2027	M28A or M25B	PENDING
M30	Phase 5	Formal System Acceptance by PSC — written approval per RFP §C.5.c	December 31, 2027	M29	PENDING

#	Phase	Milestone	Target Date	Predecessor(s)	Status
M31	Phase 5	Handoff from Implementation to Service Management — Steve Lantz as Service Manager	January 1, 2028	M30	PENDING
M32	Ops	Year 1 Operations Review — SLA performance, NOC metrics, PSC satisfaction	June 30, 2028	M31	PENDING
M33	Ops	First Annual NENA i3 Conformance Assessment — self-attestation + third-party	December 31, 2028	M31	PENDING
M34	Ops	Technology Refresh Cycle 1 — hardware EOL assessment, upgrade planning (Y3 anchor)	June 30, 2029	M31	PENDING
M35	Ops	Standards Update Review — assess impact of any new NENA i3 revisions on Nebraska	December 31, 2030	M34	PENDING
M36	Ops	Contract Year 5 Close / Renewal Planning — transition or renewal preparation	March 31, 2031	M31	PENDING
M37	Ops	Contract Term End	June 30, 2031	M36	PENDING

3.2.18.3 Master Project Gantt Chart

Figure 3.2-1 below presents the master project Gantt chart spanning the full contract period, July 6, 2026, through June 30, 2031. The implementation section (18 months) shows both cutover sequencing options at the same timeline scale. The operations section (Year 2-5) summarizes ongoing support work streams and key recurring milestones. Final dates subject to negotiation at contract kickoff.

Option A (Metro First) is presented above Option B (Pilot First) in the implementation section. The Commission will select the preferred sequencing approach at kickoff. Both options converge to the same Full Operational Status milestone of December 31, 2027.

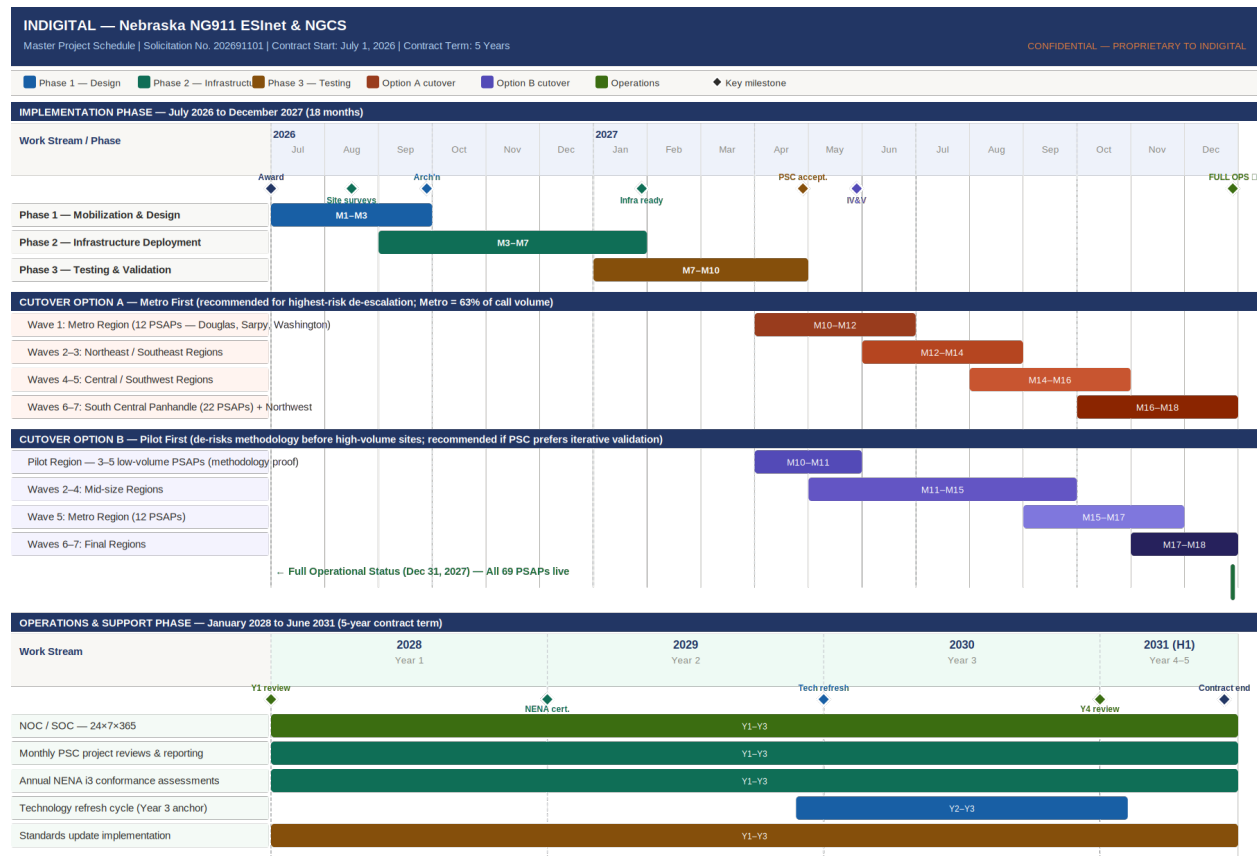


Figure 3.2-1 — Master Project Schedule, July 2026 through June 2031.

3.3 Testing and Acceptance Plan (§C.5)

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

INDIGITAL fully complies with Section C.5 of the Solicitation and explicitly accepts third-party Independent Validation and Verification (IV&V) testing of all system elements required by Solicitation 202691101. This is not qualified acceptance. We will collaborate with the PSC to establish IV&V scope and priorities, provide full system access and documentation to the IV&V evaluator, and support test execution through completion. We have nothing to hide and every incentive to pass IV&V on the first attempt.

The following represents INDIGITAL's example NG911 System Test Plan for the Nebraska deployment. This plan will be formalized post-award, refined to reflect the final Nebraska system configuration, and submitted to the PSC for written approval at least 30 days before the start of testing for any system function or component.

3.3.1 Test Environment, Facilities, and Equipment

Nebraska NG911 testing occurs in two environments. Pre-deployment functional and integration testing is conducted in INDIGITAL's dedicated lab environment, which mirrors the Nebraska production configuration and is available for PSC inspection during any test phase. Acceptance testing occurs in the live Nebraska production environment – the exact configuration that will serve Nebraska's 68 PSAPs – so that acceptance results reflect actual production performance.

Test equipment includes NENA-conformant SIP test tools capable of generating synthetic 911 call traffic, simulating PSAP positions and answering behavior, and producing position-accurate PIDF-LO location data consistent with Nebraska address points. Traffic generators are configured to simulate individual PSAPs, multiple concurrent calls from the same PSAP, and coordinated load scenarios including the 200% peak surge condition required by Section C.5.a. INDIGITAL has previously participated with IVV test programs using our MMCT (Multi-Media Call Tester) i3-ready test tooling.

3.3.2 Test Configurations and Thresholds

Baseline test configurations are defined per NENA-STA-010.3 Functional Element testing requirements and cover three operating modes: normal conditions (full-capacity, all nodes healthy), degraded-mode conditions (single-node failure, partial connectivity loss scenarios), and stress conditions at and above peak traffic. Acceptance thresholds for each test category are drawn directly from the SLA commitments negotiated post-award and include maximum call setup latency, PSAP transfer latency, GIS routing update propagation time, and ESInet availability.

Throughput acceptance testing is conducted at a sustained load of 200% of anticipated Nebraska peak call traffic for a minimum of 24 consecutive hours, as required by Section C.5.a. No element of the Nebraska system is accepted until this threshold is reached without failure. Any failure during the 24-hour window resets the clock, triggers an immediate root-cause investigation, and requires documented remediation before the test restarts.

3.3.3 Simulators and Test-Call Processes

INDIGITAL uses NENA-conformant SIP simulators to generate synthetic 911 call traffic replicating real OSP-originated scenarios, including wireless (Phase II location), VoIP, TRS/TTY text relay, and Text-to-911 call types. Each test call is assigned position-accurate PIDF-LO data consistent with a Nebraska address point, enabling ECRF routing accuracy verification at the

call level. Call flows are validated across the primary path, alternate path, and last-resort route for every PSAP in each test scenario.

3.3.4 Test Methodology: TP/TF/RTP/RTF/NA

INDIGITAL adopts the test result code methodology specified in Section C.5.c of the Solicitation. All test outcomes are documented using the following result codes, consistent with the Solicitation's definitions:

- TP (Test Passed): Requirement met; result documented with observed measured values.
- TF (Test Failed): Requirement not met; failure documented with root cause and written correction plan submitted to the PSC.
- RTP (Retest Passed): Correction verified; both the original failure record and the remediation confirmation are retained in the test log.
- RTF (Retest Failed): Correction unsuccessful; matter escalated to the PSC in writing with a revised remediation plan and revised retest schedule.
- NA (Not Applicable): Feature not applicable to the final Nebraska configuration; the basis for each NA designation is documented and reviewed with the PSC before the test phase closes.

On any failure, INDIGITAL corrects the deficit and performs regression testing to re-validate all affected tests before any component is submitted for acceptance. Results of failed tests are documented and provided to the PSC in writing. Successful regression results are delivered to the PSC before acceptance is requested for the affected component.

3.3.5 System Testing Coverage

The Nebraska test plan addresses all categories required by Section C.5.a, as shown in the following table:

Test Category	Nebraska Scope and Configuration	Result Codes
NENA-STA-010.3 Functional Element Testing	BCF, ESRP, ECRF, LVF tested against i3 interface specs. Both i3 v2 backward compatibility and i3 v3 forward path validated per Q&A #30-31.	TP / TF / RTP / RTF / NA
911 Call Flow: Primary / Alternate / Last Route	All three call paths validated for each of 68 PSAPs. Primary, alternate, and last-resort routes tested under normal and degraded-node conditions.	TP / TF / RTP / RTF / NA
End-to-End Traffic Flow	Complete path from OSP origination through ESInet,	TP / TF / RTP / RTF / NA

	NGCS routing decision, and PSAP delivery. PIDF-LO accuracy and metadata preservation verified end-to-end.	
Functional Element Interconnection	All FE-to-FE SIP and REST interface tests. Message tracing and i3 logging verification across all interface boundaries.	TP / TF / RTP / RTF / NA
Load Testing: Surge / Burst / Overflow	Unexpected surge (Metro Douglas County profile ~53% statewide volume), short burst (rural single-PSAP scale), and sustained overflow. All scenarios at 200% peak nominal load.	TP / TF / RTP / RTF / NA
ESInet Throughput and Capacity	Aggregate throughput validation across all 7 regions simultaneously. No per-PSAP degradation under full-load condition. Minimum 2 Mbps per PSAP + 2 Mbps per position (224 positions total) at 200% peak.	TP / TF / RTP / RTF / NA
ESInet Connectivity and Fault Tolerance	Failover, alternate routing, monitoring system response time, and fault notification tested. Single-node failure must not interrupt call delivery at any Nebraska PSAP.	TP / TF / RTP / RTF / NA
Security Controls	Firewall rule validation, IDS/IPS alert and block testing, mutual TLS boundary enforcement, RBAC access control verification, encryption-in-transit validation on all PSAP-facing interfaces.	TP / TF / RTP / RTF / NA

Throughput Acceptance (24+ Consecutive Hours at 200% Peak)	Mandatory continuous 24-hour run at 200% of anticipated Nebraska peak. No failures permitted during the window. Any failure resets the clock. PSC may assign observers for any portion of this test.	TP required — failure resets clock
--	--	------------------------------------

3.3.6 State Participation Rights

INDIGITAL shares all test results with the PSC project team before requesting acceptance for any component. The PSC may assign observers to any test event with reasonable advance notice; we will provide scheduling with a minimum lead time that permits observation. The PSC may inspect test equipment and applications and may require re-tests at its sole discretion. INDIGITAL will not object to reasonable re-test requirements and will provide written remediation documentation for any test event that requires PSC review before a re-test is scheduled.

INDIGITAL accepts the PSC's right to withhold final acceptance until written certification is issued. System acceptance is not self-declared. It is earned through demonstrated performance and confirmed in writing by the Commission.

3.3.7 Independent Validation and Verification (IV&V)

INDIGITAL explicitly and unequivocally accepts third-party IV&V testing of all system elements required by this procurement. Upon PSC-initiated acceptance testing completion, the State will conduct IV&V using a third-party evaluator. INDIGITAL will collaborate with the PSC and the IV&V evaluator to establish scope and priorities, provide access to all system documentation, configuration baselines, and interface specifications, and support test execution throughout the IV&V process. INDIGITAL will supply on-site or remote technical support to the IV&V team at no additional cost to the Commission.

3.4 Training Plan (§E.7)

The Contractor shall provide training to ensure that PSAP operators, administrators, and Commission staff can effectively operate, manage, and oversee the deployed NG911 ESInet/NGCS system. Consistent with Section B.7 of the Solicitation, INDIGITAL shall provide operator and administrator manuals, training materials, and runbooks required for all user classes.

INDIGITAL fully complies with the training requirements of the Solicitation. Our training program is structured around three distinct user populations, each with different operational responsibilities and different levels of technical depth. We do not deliver generic vendor training built around product features. We develop Nebraska-specific training content that reflects the actual Nebraska system configuration, actual Nebraska PSAPs, and actual Nebraska call flow scenarios.

3.4.1 PSAP Operator Training

PSAP operator training prepares dispatch and call-handling personnel to use the NG911-connected system confidently from day one of cutover. Content covers call receipt and answering, call transfer with metadata and location preservation, Text-to-911 and multimedia call handling, overflow and backup routing behavior, system status indicators, and emergency procedures for anomaly conditions. No operator handles a live Nebraska 911 call on the new system without completing this training first. Training is scheduled at each PSAP prior to its cutover date in the phased rollout sequence.

Our training program is designed to be flexible and available to support complicated 24x7 operations at the PSAP. Our recommendation is to do a mixture of regional PSAP Director and Assistant Director Level training, and PSAP-specific training in person at each PSAP to support Telecommunicator Training needs.

Additionally, INDIGITAL provides virtual training through a series of videos and guided documentation to help support ongoing training needs. Lastly, INDIGITAL includes Market and Service managers dedicated to the Nebraska project to assist with any additional training needs.

Delivery format: In-person on-site or regional-cluster sessions, with virtual LMS access for shift staff who cannot attend in-person sessions.

3.4.2 System Administrator Training

PSAP system administrator training covers all configuration management capabilities available to PSAP-level administrators: user account provisioning and access control management, reporting dashboard access and export, alarm acknowledgment and escalation procedures, routine maintenance tasks, and coordination with INDIGITAL's NOC for issue reporting and escalation. Administrator training includes hands-on lab time in a training environment that mirrors the Nebraska production configuration before any changes are made in production.

Documentation provided with administrator training: System Administrator Manual, configuration reference guide, troubleshooting runbook, and a quick-reference card for common administrative tasks.

3.4.3 Commission Staff Training

PSC staff training addresses system oversight capabilities rather than call handling. Content covers the statewide operational status dashboard, CDR access and custom reporting, commission-level analytics integration (per Addendum 2, Q&A #27), escalation procedures for service events, and how to initiate a formal Change Request or issue report through INDIGITAL's project management process. The goal is an empowered PSC: Commission staff who can independently verify system performance, pull their own reports, and initiate action without waiting for INDIGITAL to surface information.

3.4.4 Training Deliverables

INDIGITAL will produce and deliver the following training deliverables in support of the Nebraska NG911 deployment. Each deliverable aligns with the requirements of RFP §E-7 and the deliverables table in Volume 2, Section 2.9. All materials are delivered in editable digital format so the Commission can maintain, customize, and reuse them for ongoing personnel training throughout the contract term.

3.4.4.1 Training Plan and Sample Materials (RFP §7.8)

A comprehensive training plan covering all audiences and topics identified in §E-8.1 and §E-8.2, including PSAP operations personnel, state-level operations staff, and system administrators. The plan defines curriculum structure, session scheduling, delivery methods (in-person, virtual, and self-paced), and role-based training tracks. Sample documentation and instructional materials accompany the plan for State review and approval prior to delivery.

3.4.4.2 Train-the-Trainer (TtT) Curriculum (RFP §7.5)

A complete TtT curriculum package designed for State-designated trainers to independently deliver PSAP operator and administrator training after initial deployment. The curriculum includes instructor guides, lesson plans, presentation decks, hands-on lab exercises, and answer keys. All TtT materials are submitted for State approval and maintained in current versions for the duration of the contract.

3.4.4.3 PSAP Operator Quick-Start Guide

A Nebraska-specific quick-reference guide covering day-one essential tasks: login and logout procedures, password reset, equipment problem reporting, call transfer, call conferencing, discrepancy reporting, foreign language interpretation processes, rebid and refresh of call information, instant recorder and playback, Text-to-911 (T2911) operations, and Text-from-911 (T-from-911) operations, per the minimum training elements in RFP §7.2.

3.4.4.4 PSAP Operator Full Reference Manual

A comprehensive reference manual covering all NGCS call-handling features, CPE integration points, network status reports, help desk usage and processes, trouble ticketing, and advanced operational scenarios. This manual serves as the primary day-to-day resource for PSAP telecommunicators and supervisors.

3.4.4.5 System Administrator Manual

A technical reference for network administrators and IT staff responsible for system configuration, monitoring, and maintenance. Content includes user account management, system health dashboards, alarm and event interpretation, GIS update procedures, ECRF/LVF provisioning, ESInet connectivity monitoring, failover procedures, and change management protocols.

3.4.4.6 Commission Staff Oversight and Reporting Guide

A guide tailored for Nebraska 911 Commission personnel covering statewide system monitoring, performance reporting, SLA compliance tracking, root-cause analysis review processes, and administrative oversight functions. This deliverable ensures Commission staff can independently verify system performance against contractual commitments.

3.4.4.7 Emergency Procedures Runbook

Step-by-step procedures for system anomaly response, failover activation, disaster recovery scenarios, and escalation protocols. The runbook addresses both localized PSAP-level incidents and statewide service disruptions, with defined roles, notification chains, and recovery verification steps.

3.4.4.8 Comprehension Testing and Certification Materials (RFP §7.7)

A full assessment package supporting the testing and certification requirements of §7.7. Materials include written examination question banks, oral examination guidelines, hands-on practical testing scenarios, scoring rubrics, and end-of-course certification templates. Testing is applied at intervals during initial and ongoing training, with a final evaluation of each student's knowledge provided to the State upon course completion.

3.4.4.9 Post-Deployment Training Materials (RFP §7.6)

A standalone training package designed for post-deployment refresher and new-hire training sessions accommodating up to fourteen (14) students per class. This package includes all instructor materials, student workbooks, and lab exercises required for classroom delivery, as well as the post-deployment TtT course materials with defined maximum class size.

3.4.4.10 Application-Specific Training Materials

Dedicated training materials for supplemental applications deployed as part of the Nebraska solution, including Texty (Text-to-911 and Text-from-911 management) and MEVO (multimedia evidence and voice operations), as applicable to the project scope.

3.4.4.11 Scheduling and Logistics Documentation (RFP §7.4)

A training schedule and logistics plan confirming delivery of all training no later than fourteen (14) calendar days before each PSAP cutover, identification of temporary training site(s) within Nebraska, and availability of weekend and evening sessions to accommodate call-taker schedules and maintain the deployment timeline.

All materials are provided in current versions at system acceptance. Updated versions are delivered with each major software release and maintained at the State for the duration of the contract per §7.5.

VOLUME 4: Response To Technical Requirements

4.1 ESInet Technical Narrative (§E.1)

RFP §E.1: 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 PSTN and SIP, diverse physical routing paths, and network-level redundancy that eliminates any single point of failure.

INDIGITAL fully complies with all requirements set forth in RFP §E.1 ESInet Requirements. Our proposed Emergency Services IP network (ESInet) is architected from the ground up to the NENA-STA-010.3-2021 (i3) Standard and designed to serve all 68 Nebraska PSAPs across 7 regions from day one of operational readiness.

4.1.1 Architecture and Topology (§E.1.1)

INDIGITAL's ESInet architecture is a fully managed, multi-tenant IP emergency services network built on a geographically diverse, redundant core. The design eliminates every single point of failure at the link, router, server, and data center levels, delivering the sub-second failover Nebraska's 68 PSAPs require across 7 service regions.

The ESInet interconnects all NG911 functional components — PSAPs, Originating Service Providers (OSPs), Next Generation Core Services (NGCS), and adjacent ESInets — using Internet Protocol over a managed backbone, with legacy interface support for any PSAPs or OSPs not yet on full IP transport. Our architecture natively supports both IPv4 and IPv6 in a dual-stack configuration, ensuring seamless interoperability with the full spectrum of current and next-generation endpoints Nebraska will encounter across its 7-region, 68-PSAP deployment.

Virtual routing instances and logical traffic segregation enforce strict separation of emergency services traffic from non-emergency traffic on all shared infrastructure. Emergency signaling and media streams are isolated at the network layer and cannot be disrupted by or commingling with other tenants or operational traffic.

INDIGITAL's IP addressing, VLAN segmentation, VRF isolation, and DiffServ QoS policy design are illustrated in Volume 2, Figure 2.2-2. The diagram demonstrates our approach to logical network segmentation between the Omaha and Lincoln core nodes, including dedicated subnets per data center, VRF-based traffic isolation between emergency and non-emergency services, out-of-band management VLANs, and DSCP marking assignments that enforce strict priority queuing for 9-1-1 signaling and media per NENA-STA-010.3 packet marking specifications. Refer to Section 2.2 for the complete QoS policy narrative and DiffServ mapping table.

4.1.1.1 Multi-Tenant and Interconnect Design

Our ESInet supports multi-tenant interconnects with both the Public Switched Telephone Network (PSTN) and Session Initiation Protocol (SIP) endpoints. Carrier peering is established through standards-based Border Control Functions (BCFs) with documented procedures, APIs, and configuration templates for peering with adjacent ESInets, third-party providers, and legacy

networks. Border Gateway Protocol (BGP) is used as the sole Exterior Gateway Protocol (EGP) for all multi-site reachability and load distribution, per RFP §E.1.1 requirements.

We provide complete documentation packages for each OSP interconnect, including policy-based routing rules and traffic-exchange agreements. All OSP interfaces support both location-by-reference and location-by-value conveyance to ensure seamless integration across the diverse OSP landscape Nebraska's statewide deployment will encounter.

4.1.1.2 Redundancy and Failover

INDIGITAL's ESInet incorporates geographically diverse redundant network cores with duplicate session border and edge elements at every tier. Automatic, transparent failover for both signaling and media is implemented at every level: link, router, server, and data center. Failure of any single component — including a link, router, or server — does not disrupt 911 service to any Nebraska PSAP.

Our architecture guarantees a **Recovery Point Objective (RPO) of less than one (1) minute** and a **Recovery Time Objective (RTO) of less than five (5) seconds** for all critical signaling and media paths. We deploy active-active configurations across data centers separated by a minimum of 100 miles, with active-passive standby available for components where active-active is not architecturally appropriate. For each such component, we document the detection mechanism and worst-case failover timeline.

4.1.1.3 SIP, TLS, and Media Security

All ESInet signaling uses Session Initiation Protocol (SIP) per RFC 3261 and applicable NG911 SIP extensions. Signaling is transported exclusively over SIP over Transport Layer Security (TLS), and all media is carried over Secure Real-time Transport Protocol (SRTP). Standard transports — TLS over TCP and UDP where applicable — are supported in full IPv6 compatibility alongside IPv4, meeting the RFP's dual-stack requirements at every interface.

4.1.1.4 ESInet Architecture Diagrams

Comprehensive network diagrams — including logical topology, physical topology, inter-data-center connectivity, OSP peering points, PSAP connection architecture, and BCF placement — are provided in the supporting exhibit to this volume. All diagrams are maintained in a configuration management database accessible to the Nebraska 911 Advisory Committee and PSC at any time during the contract term. Diagrams are updated within 5 business days of any architecture change and version-controlled with change history.

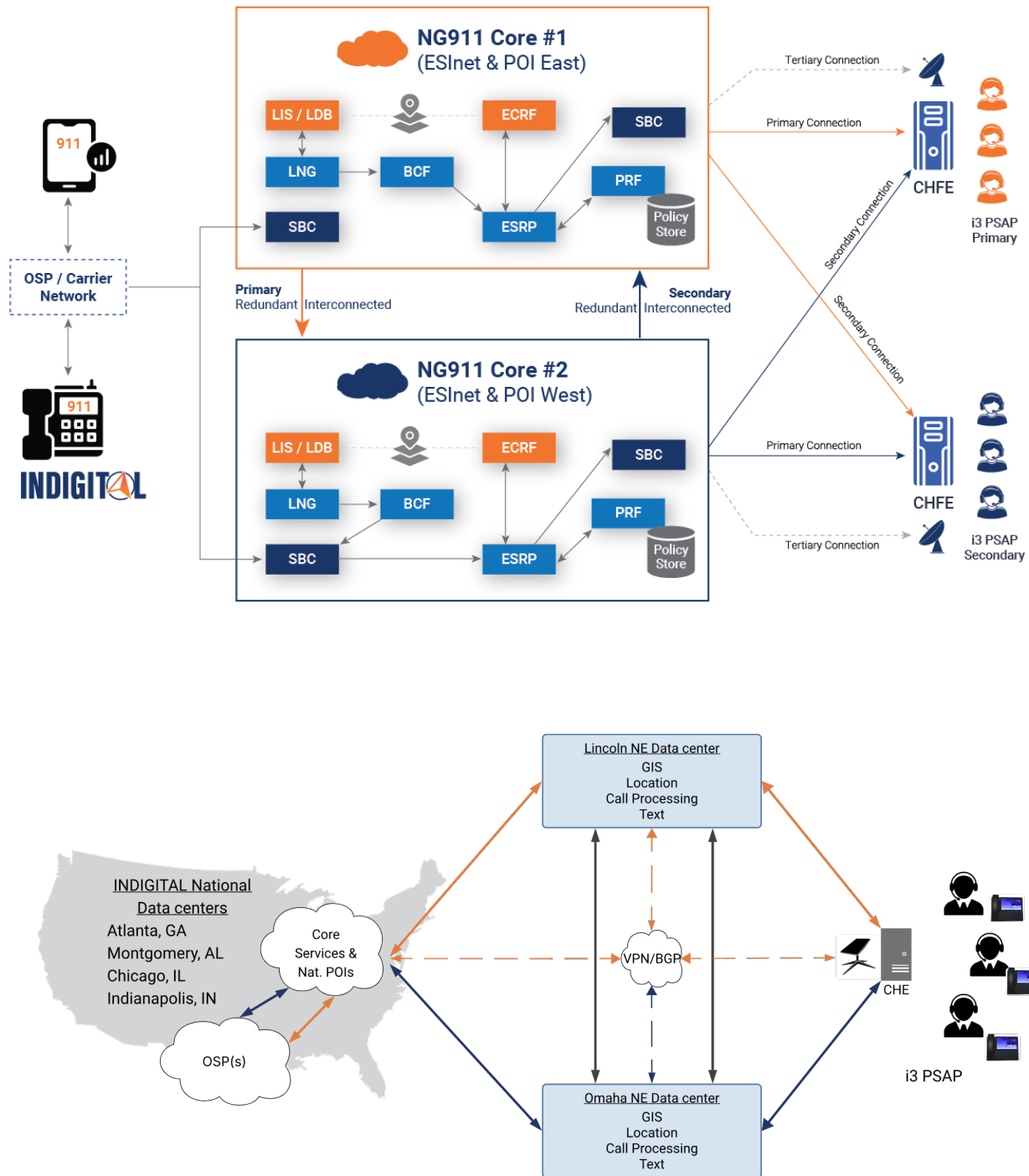


Figure 4.1-1 and -2: NG911 Core Redundancy Architecture

This diagram illustrates INDIGITAL's active-active, dual-core ESInet design for Nebraska, with geographically diverse data centers in Lincoln and Papillion. Each core operates independently with fully redundant NGCS functional elements – including BCF, ESRP, ECRF, LVF, and Policy Store – ensuring seamless failover and continuous 911 service delivery across all 68 Nebraska PSAPs.

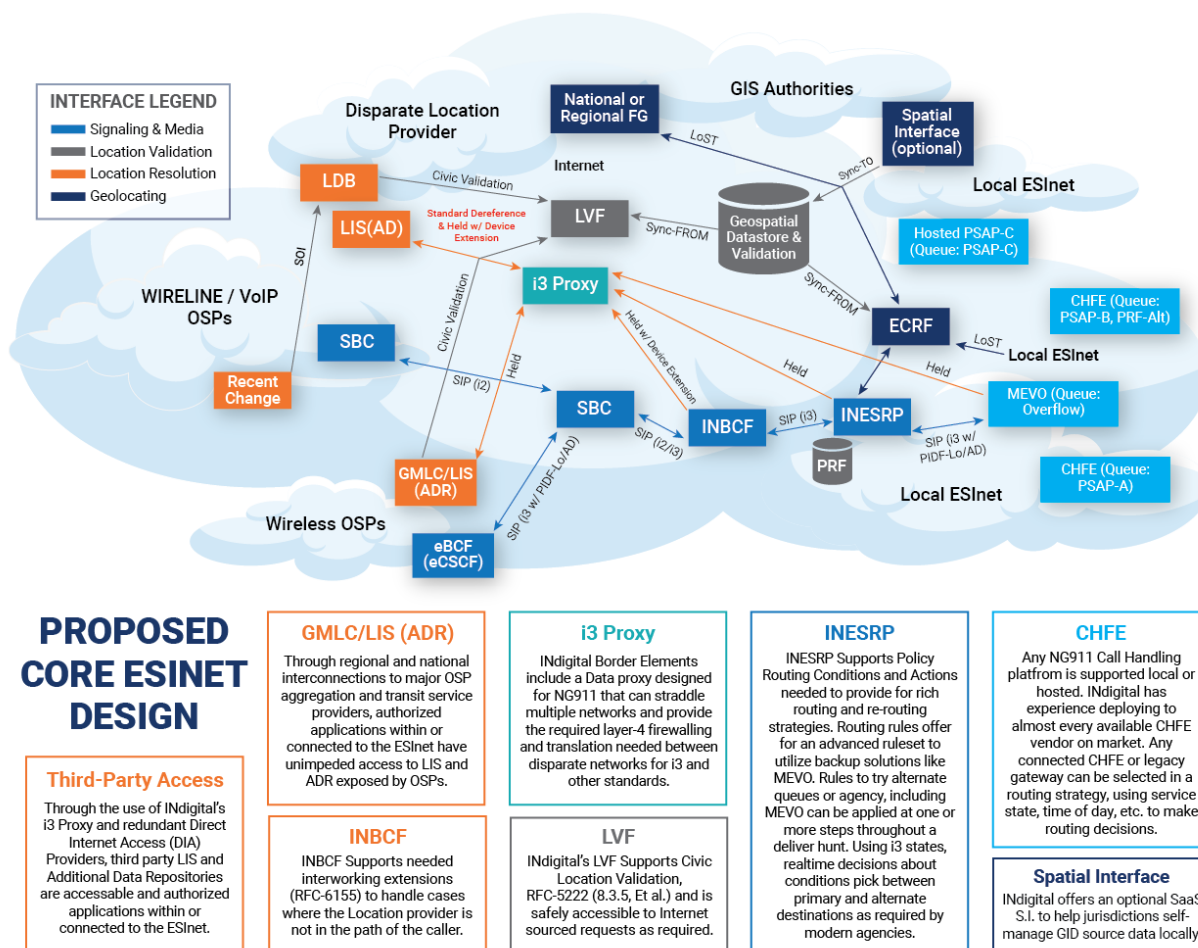


Figure 4.1-3: Proposed Core ESInet Design

This diagram presents INDIGITAL's proposed core ESInet architecture for Nebraska, illustrating the complete signaling and media path from originating service providers through the ESInet to PSAP delivery. Wireline/VoIP and wireless OSPs connect through SBCs and i3 Proxies to the NGCS core, where the INBCF handles interworking extensions, the INESRP performs policy-based routing using the PRF and Policy Store, and the ECRF/LVF resolves location for routing decisions. The LDB and LVF provide civic validation and location resolution services. CHFEs at local ESInets deliver calls to primary, backup, and overflow PSAP queues. Third-party access through i3 Proxy and redundant DIA providers ensures that authorized LIS and ADR applications have unimpeded connectivity to the ESInet.

4.1.2 External and PSAP Connectivity (§E.1.2)

4.1.2.1 Originating Service Provider (OSP) Connections (§E.1.2.1)

INDIGITAL maintains production interconnections with all major OSPs operating in NG911 environments, including AT&T, Intrado, Motorola Solutions Network, and NGA. Our ESInet provides documented, standards-based IP Points of Interconnection (POIs) for all Nebraska OSPs. Each POI is supported by a configuration template, tested interconnect procedures, and a formal traffic exchange agreement.

All OSP interfaces support the standard SIP signaling extensions defined in NENA-STA-010.3 Table 1, including PIDF-LO location conveyance in both location-by-reference (LbyR) and location-by-value (LbyV) formats.

INDIGITAL maintains interconnection agreements with all major OSPs throughout the United States. INDIGITAL may be required or may require updated documents to specifically address Nebraska projects' needs.

4.1.2.2 PSAP Connections (§E.1.2.2)

Each of Nebraska's 68 PSAPs — 12 host sites and 57 remote sites across 7 regions — receives a dedicated, managed IP circuit to the INDIGITAL ESInet. Bandwidth is provisioned at a minimum of 2 Mbps per PSAP plus 2 Mbps per position, scaled to 200% of anticipated peak call volume. For Nebraska's 224 total positions, this yields a baseline of 2 Mbps + (224 × 2 Mbps) = 450 Mbps total position-based capacity, sized to 200% peak.

PSAP connections are engineered with diverse physical routing paths and automatic failovers. Each host PSAP receives redundant circuits from diverse physical paths. Remote PSAPs are connected through their host site with appropriate redundancy for the remote link segment. No PSAP connection relies on a single physical path for continuity of 911 service.

4.1.3 Legacy Interoperability (§E.1.3)

INDIGITAL's ESInet provides full legacy interoperability through three gateway function classes, aligned to RFP §E.1.3 requirements and NENA-STA-005.2:

- Legacy Network Gateway (LNG, §E.1.3.1): Bridges legacy PSTN trunks to the ESInet IP backbone. Implements the same stringent security, logging, monitoring, and redundancy requirements as all other ESInet functional elements.
- Legacy Selective Router Gateway (LSRG, §E.1.3.2): Enables interoperability with legacy selective routers still in operation during the Nebraska transition period, including any LSRGs required for the 5 OSPs with June 2026 extension dates and Hamilton TRS through end of 2026.
- Legacy PSAP Gateway (LPG, §E.1.3.3): Supports PSAPs that have not yet transitioned to NG911 CHE, providing a migration bridge that allows legacy endpoints to receive 911 calls through the INDIGITAL ESInet without disruption.

All three gateway types are deployed with the same active-active or active-passive redundancy architecture as the core ESInet, ensuring that legacy interoperability does not introduce single points of failure.

4.1.4 Network Performance (§E.1.4)

4.1.4.1 QoS and Traffic Prioritization

INDIGITAL's ESInet enforces Differentiated Services (DiffServ) QoS policies across all network nodes, with configurable DSCP markings that prioritize 911 signaling (SIP INVITE transactions and related SIP messages) and media streams above all other traffic classes. Emergency voice is engineered to maintain a Mean Opinion Score (MOS) greater than 4.0 under all load conditions, including during simulated peak scenarios equivalent to 200% of Nebraska's anticipated peak call volume of approximately 954,417 annual calls statewide.

Traffic policing and shaping mechanisms prevent any single traffic class from consuming disproportionate bandwidth and triggering congestion that could degrade 911 voice quality. Automated congestion management activates before voice quality degradation occurs.

4.1.4.2 Bandwidth Provisioning (§E.1.4.2)

All ESInet links are provisioned at a minimum of 200% of anticipated peak call volume, per RFP §E.1.4.2. Nebraska's statewide traffic profile – with the Metro region carrying approximately 63% of volume and Douglas County carrying approximately 53% is used as the baseline for per-region capacity planning. Scalable bandwidth architecture allows capacity to be increased without service interruption as call volumes or PSAP deployments change over the 5-year contract term.

4.1.4.3 Network Time (§E.1.4.6)

Nebraska Data Centers and **National Data Centers** will utilize redundant Stratum 1 hardware clocks that support IEEE Std. 1588-2008 (PTP) and RFC-5905 (NTP), with over 24 hours of holdover in isolation. These clocks are Time synchronized to a centralized master Stratum 1 hardware clock with GPS located at the Fort Wayne National Data Center. All clocks will utilize a public NIST NTP server in the advent of isolation from the master clock.

- **Hypervisor Hosts** will use PTP for synchronizing hardware clocks within the infrastructure.
- Network Appliances and Guest VMs will support NTP.

Time accuracy is maintained within ± 1 millisecond across all network elements, ensuring consistent timestamping for call records, security events, and system logs across all seven Nebraska regions.

4.1.5 Resilience and Service Levels (§E.1.5)

4.1.5.1 Availability (§E.1.5.1)

INDIGITAL commits to 99.999% availability for all core voice paths within the ESInet. This SLA is maintained across active-active data center configurations, with automatic failover ensuring that failure of any single data center does not reduce call processing capability below full operational capacity.

4.1.5.2 Router Diversity and Reliability (§E.1.5.2)

INDIGITAL's ESInet reliability design conforms to RFP §E.1.5.2 and the requirements confirmed in Addendum 2, Q&A #11. At every ESInet node, we deploy at least two physical network routers from different manufacturers, providing equipment and vendor diversity that eliminates any

single-vendor router failure mode. This dual-manufacturer approach ensures that a firmware defect, hardware recall, or vendor-specific vulnerability affecting one router platform does not simultaneously impair both routing paths at any node.

Strategic diversity is implemented across three axes: geographic regions, technology platforms, and router manufacturers. This tri-dimensional diversity approach ensures that no combination of geographically correlated events, technology-specific failure, and vendor-specific defect can simultaneously disable redundant routing paths at any single node.

The reliability design conforms to FCC Report and Order 13-158 for enhancing 911 reliability across all communication networks. No segment of the Nebraska ESInet relies on a single physical path, a single routing platform, or a single data center. The 'backhoe incident' scenario — loss of a single fiber path — is fully mitigated through diverse physical routing at every segment.

4.1.5.3 Multivendor diversity:

4.1.5.4 Cisco

- **Role:** Primary vendor for routing and switching infrastructure.
- **Expertise:** INDIGITAL has extensive experience with Cisco products, supported by a team of technicians proficient in their deployment and management.
- **Reliability:** Cisco routers ensure robust route paths, contributing to overall system reliability and compliance with FCC standards.

4.1.5.5 Arista

- **Role:** Alternate vendor for routing and switching solutions.
- **Strengths:** Known for high-performance networking capabilities, Arista provides additional redundancy and flexibility in system architecture.
- **Integration:** Their hardware complements Cisco offerings, enhancing overall network resilience and performance.

4.1.5.6 Fortinet

- **Role:** Alternate vendor focused on security and network appliances.
- **Features:** Fortinet's products strengthen INDIGITAL's security posture, addressing vulnerabilities and providing essential protection for network infrastructure.
- **Collaboration:** Works alongside Cisco and Arista to create a comprehensive and secure networking environment.

4.1.6 Operations and Management (§E.1.6)

4.1.6.1 Network Operations Center (§E.1.6.1)

INDIGITAL operates a dedicated 24x7x365 Network Operations Center (NOC) providing continuous monitoring of all ESInet components across Nebraska's 7 regions. NOC provides real-time operational dashboards, threshold-based alerting, historical trend analysis, and integration with external monitoring tools via APIs.

The ESInet monitoring platform includes: a Network Management System (NMS) with real-time performance dashboards; SNMPv3 polling and trap collection from all monitored elements; syslog aggregation and analysis; and key performance indicator (KPI) tracking for latency, packet loss, jitter, and availability at each circuit and node. All monitoring data is retained for the contract term and is accessible to PSC through a web-based portal.

NOC staffing, escalation tiers, and the detailed incident response procedures meeting RFP §E.9.3.1 minimum NOC requirements are addressed in Volume 2 Section 2.9 (Service Management Framework) and Volume 3 Section 3.1 (Project Management Approach).

4.1.6.2 Maintenance Windows (§E.1.6.2)

All planned maintenance activities are coordinated with the Nebraska PSC at least 10 business days (14 calendar days), in advance. Maintenance windows are scheduled during off-peak periods (nominally 2:00 AM to 5:00 AM local Nebraska time) and are never scheduled during periods of elevated call risk (severe weather watches, major public events, or PSC-declared high-risk periods). All maintenance is performed in a manner that maintains 99.999% availability — no maintenance window may reduce call handling capacity below full operational levels.

4.1.6.3 Implementation Details and Port Mapping (§E.1.7)

Complete port mapping documentation — including all required TCP/UDP ports for ESInet interfaces, OSP connections, PSAP connections, and management plane — is provided in the technical appendix to this volume. Port mapping is maintained in the configuration management database alongside the network topology diagrams and is updated with each architectural change.

4.1.7 ESInet Interconnection with Neighboring States (§E.1.1.2)

Upon deployment, INDIGITAL's Nebraska ESInet provides seamless IP interconnections with neighboring state ESInets. BGP peering arrangements with adjacent state emergency services networks are established using documented interconnect procedures and tested prior to cutover. Newly established ESInets in cooperating states are able to connect to the Nebraska State ESInet within a designated timeframe. All networks interconnecting with the Nebraska ESInet meet the minimum security and performance qualifications for interconnection. The State's security posture is collaboratively maintained with all connected network providers through shared threat intelligence, coordinated incident response, and network security requirements applied uniformly at every interconnect point.

4.2 NGCS Technical Narrative (§E.2)

RFP §E.2: The proposal must include a Next Generation Core Services (NGCS) implementation deployed across multiple redundant data centers. The contractor shall supply or ensure interoperability with all NGCS functional elements as defined by NENA, including but not limited to the LVF, LIS, ECRF, ESRP, BCF, ADR, and Logging Service.

INDIGITAL fully complies with RFP §E.2 NGCS requirements. Our NGCS is a complete, production-deployed NG911 core services stack aligned to NENA-STA-010.3-2021 (i3 Standard), with every required functional element implemented and operational. Nebraska's 68 PSAPs receive a proven NGCS platform — not a platform-in-development or a third-party integration arrangement — from a vendor that has operated comparable statewide NG911 infrastructure.

4.2.1 Architecture and Data Center Deployment (§E.2)

INDIGITAL's NGCS is deployed across a minimum of three (3) redundant data centers, meeting the RFP §E.2 architecture requirements. Data center placement includes a preference for at least one in-state Nebraska facility and at least one geographically distant facility more than 100 miles away, with a third facility providing additional geographic and jurisdictional diversity. Every NGCS component — physical and virtual — is redundantly deployed across all data centers, with no single point of failure in any component or inter-component path.

The Nebraska NGCS instance is architecturally isolated from other INDIGITAL customer deployments. Incidents, outages, or security events in other ESInet or statewide NGCS services operated by INDIGITAL cannot propagate to or impact Nebraska's NGCS. Isolation is enforced at the network layer (separate VLANs, firewalls, and routing domains) and at the application layer (separate policy stores, certificate authorities, and logging repositories).

4.2.1.1 Failover and State Management

For every NGCS functional element, we document whether it operates in active-active or active-passive configuration. For active-active elements, we describe how clients detect element failure and recovery, including the worst-case recovery time. For each database and call-state data object, we describe how state is reliably maintained during failover, including replication strategy, maximum data sync time, and the mechanism for achieving it. For databases updated at call time, replication strategy, maximum data sync time, and recovery are documented and committed to in the SLA framework.

Dynamic ECRF service boundary polygon updates are fully supported. When the PSC or an authorized PSAP updates a service boundary polygon in the ECRF, replication of that update across all active ECRF instances completed within the timeframe committed to in our SLA. The replication mechanism, monitoring, and verification process for polygon updates are described in the technical appendix.

4.2.2 Edge Security and Ingress (§E.2.1)

4.2.2.1 Border Control Function (BCF, §E.2.1.1)

INDIGITAL's BCF serves as the security and policy enforcement boundary between the ESInet and all external network connections, including OSP connections, PSAP connections, and adjacent ESInet peering points. The BCF implements mutual TLS authentication, SIP message validation, rate limiting, and policy-based access control for all ingress and egress traffic. It

provides the primary defense against SIP-based threats, including SIP flooding, spoofing, and injection attacks.

BCF instances are deployed redundantly across all data centers in an active-active configuration, ensuring that failure of a single BCF instance causes no service disruption. BCF policy rules are version-controlled and change-managed, with all policy changes logged and attributable to an authorized identity.

4.2.2.2 STIR/SHAKEN Support (§E.2.1.2)

INDIGITAL's NGCS implements STIR/SHAKEN (Secure Telephony Identity Revisited / Signature-based Handling of Asserted information using toKENs) per ATIS and IETF standards. The NGCS validates PASSporT tokens on inbound calls and passes attestation data to PSAPs as part of the call metadata.

4.2.2.3 Security Mechanisms (§E.2.1.3)

In addition to BCF-layer defenses, INDIGITAL's NGCS implements NENA-defined security mechanisms at every internal component interface. All inter-component communication uses mutual TLS. Role-Based Access Control (RBAC) governs all management plane access. Session hijacking and replay attack protections are implemented at every SIP interface. All threat mitigation measures are documented in the Security Technical Narrative (Section 4.4) and the Security Technical Appendix.

4.2.3 Core Routing and Location (§E.2.2)

4.2.3.1 Emergency Services Routing Proxy (ESRP, §E.2.2.1)

INDIGITAL's ESRP provides location-based routing for all 911 calls entering the Nebraska NGCS. The ESRP queries the ECRF to determine the correct PSAP for each call based on the caller's location, applies policy rules from the Policy Store, and routes the call to the appropriate PSAP or default routing destination if authoritative GIS routing is unavailable. SIP header preservation is maintained through the ESRP so that all call metadata – including PIDF-LO location, ANI/ALI data, and call source information – is delivered to the PSAP CHE intact.

4.2.3.2 Policy Store (§E.2.2.1.1)

All NGCS elements that use policies retrieve those policies from a NENA-STA-010.3-compliant policy server. Each element is provisioned with the host name of its policy server and retrieves updated policies on a defined schedule. Policy updates – including changes to service boundary routing, PSAP queue management, and call overflow rules – are applied without service interruption and without requiring system restarts.

4.2.3.3 Location Information Server — LIS Interface (§E.2.2.2)

Per Addendum 2, Q&A #23 clarification, the Nebraska NGCS fully supports the NENA i3 LIS interfaces used to retrieve location from i3-compliant OSPs and other access network providers. INDIGITAL does not propose deploying a full LIS within Nebraska's access network – the LIS is an OSP function. Our NGCS implements the standardized LIS query interface (using the HELD protocol per RFC 5985 and LoST per RFC 5222) to retrieve location data from any i3-conformant LIS in the OSP network, ensuring accurate location-based routing for all call types.

4.2.3.4 Location Database (LDB, §E.2.2.3)

The INDIGITAL NGCS includes a Location Database that maintains address and location records for use in call routing and ALI/MSAG-equivalent functions. The LDB is synchronized with the ECRF GIS data repository and is updated on the same schedule as the ECRF — within 5 minutes of any routing-impacting GIS change. The LDB supports both legacy MSAG/ALI-format data (for backward compatibility with i3 v2 CHE) and NENA GIS Data Model format (for i3 v3 and forward).

4.2.3.5 ECRF and LVF (§E.2.2.4)

INDIGITAL's Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) use authoritative GIS data in the NENA GIS Data Model format (NENA-STA-006.2-2022) to determine the correct PSAP for every 911 call. The ECRF supports LoST protocol queries (RFC 5222) and returns the correct Emergency Service Number (ESN) and PSAP routing URI for any valid location query within Nebraska.

The LVF validates caller location data on inbound calls, checking it against the authoritative GIS boundaries to confirm that the reported location falls within a recognized service area. Invalid or unresolvable locations trigger defined fallback routing rules that route the call to the appropriate default PSAP while flagging the location data quality issue for GIS team follow-up.

The 5-minute GIS propagation SLA — confirmed in Addendum 2, Q&A #11 — is met through INDIGITAL's Data Integrity Gateway (DIG), which acts as the Spatial Interface and pushes validated GIS data updates into the ECRF and LVF in near real time. The 5-minute clock starts when data is verified and presented to core services by the DIG. Additionally, once a validated dataset is presented to the ECRF by the Spatial Interface, INDIGITAL's DIG-to-ECRF propagation completes within eight seconds, well within the requirement in RFP §E.2.2.4. GIS data management is addressed in detail in Section 4.3.

4.2.3.6 Forest Guide (§E.2.2.5)

INDIGITAL's NGCS includes a Forest Guide function that maintains the namespace mapping for the Nebraska ESInet, enabling ESRP queries to resolve PSAP URIs across all routing domains in the state. The Forest Guide is synchronized with all ECRF instances and updated whenever PSAP service boundaries or routing URIs change.

4.2.3.7 Service/Agency Locator (SAL, §E.2.2.6)

The Service/Agency Locator provides a centralized directory for all agencies and service providers within the Nebraska ESInet. The SAL supports PSAP discovery, transfer routing, and agency federation within the i3 framework.

4.2.4 Data and Enrichment (§E.2.3)

4.2.4.1 Additional Data Repository (ADR, §E.2.3.1)

INDIGITAL's ADR stores and serves supplementary call-related data — including subscriber data, device data, and agency-specific data — that enriches 911 calls with context beyond the basic call and location record. The ADR exposes standardized RESTful APIs (JSON/XML payloads per NENA-STA-010.3 specifications) for data submission by authorized agencies and for retrieval by PSAPs at call time. All ADR data is encrypted at rest and access-controlled per the RBAC policy framework.

4.2.5 Call Flow and Media Handling (§E.2.4)

4.2.5.1 i3 Call Flows and SIP Header Preservation (§E.2.4.1)

INDIGITAL's NGCS implements the complete i3 call flow architecture defined in NENA-STA-010.3, including emergency call origination, routing, PSAP delivery, transfer, conference, and callback. All SIP headers are preserved and forwarded intact through every element in the call path – BCF, ESRP, and PSAP delivery – including PIDF-LO location data, call source information, ANI/ALI equivalents, and any additional data references.

INDIGITAL supports both i3 Version 2 backward interoperability and i3 Version 3 forward migration, as required by RFP §E and clarified in Addendum 2, Q&A #30 and #31. Backward interoperability with i3 v2 is implemented at the CHE and OSP interfaces, allowing PSAPs with i3 v2 CHE to receive calls with full location and call data without requiring CHE upgrades at cutover. The forward migration path to i3 v3 is implemented within the NGCS itself, ensuring Nebraska is not locked into a single i3 version as NENA standards evolve.

I3 version 3 builds adds functionality to previous version 2 but is not an architectural change between standards. Some of these enhancements include call handling improvements, for call bridging, blind transfer support and improved call control features (future IoT, Advanced Automatic Crash Notification (AACN)). Additional functionality in v3 also introduced the OCIF, more structure around discrepancy reporting, API driven ecosystem, enhanced cybersecurity framework, integrations using REST/JSON, and matured trust frameworks to name a few.

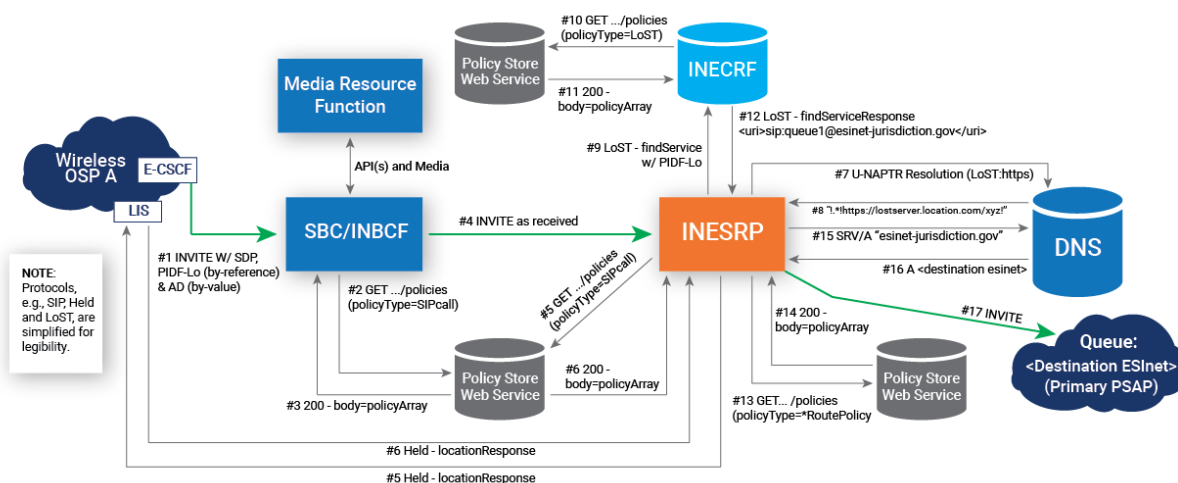


Figure 4.2-1: NENA i3 Call Flow Sequence

This diagram traces the 17-step call flow for a wireless emergency call through INDIGITAL's NGCS. The sequence begins with a SIP INVITE from the wireless OSP (Step 1), passes through the SBC/INBCF for border control and policy evaluation (Steps 2-6), proceeds to the INESRP for location-based routing (Steps 4-6), which queries the INECRF via LoST protocol for PSAP resolution (Steps 7-12). The INESRP applies route policies from the Policy Store (Step 13), resolves the destination ESInet via DNS (Steps 14-16), and delivers the INVITE to the primary PSAP queue (Step 17). Location is obtained via HELD protocol from the Media Resource Function and dereferenced at both the SBC/INBCF and INESRP stages. All policy lookups,

including SIP call policies and LoST routing policies, are retrieved from distributed Policy Store Web Services.

4.2.5.2 Multimedia Support (§E.2.4.2.1)

INDIGITAL's NGCS supports multimedia emergency communications, including voice (SIP-based), text (Real-Time Text per RFC 4103 and NG911 TCC integration), and video (SIP-based video calls for video-capable PSAPs). All media types are handled through the same i3 call flow architecture, with PIDF-LO location delivery and SIP header preservation maintained for all media types.

4.2.5.3 Media Quality of Service (§E.2.4.2)

Media QoS within the NGCS is enforced through DSCP markings, priority queuing, and traffic shaping at every media path element. Voice quality is maintained at MOS > 4.0 under all load conditions. Media QoS policies are aligned with ESInet-level QoS policies to provide end-to-end priority enforcement from OSP ingress to PSAP delivery.

4.2.5.4 Interactive Multimedia Response Service (IMRS, §E.2.4.3)

INDIGITAL's NGCS supports the Interactive Multimedia Response Service function for pre-PSAP call handling and queuing. IMRS provides overflow handling, pre-announcement, and queue management during periods when all PSAP positions are occupied.

4.2.5.5 Bridge (§E.2.4.4)

INDIGITAL's NGCS includes a conference bridge function supporting multi-party 911 calls, including emergency responder conferencing, PSAP transfer with metadata preservation, and supervisor monitoring. All bridge sessions preserve the full call metadata — including location, caller identity, and call history — for all parties throughout the session.

4.2.6 Legacy Bridging (§E.2.5)

INDIGITAL's NGCS supports bridging legacy systems through appropriate gateways, including MSAG/ALI legacy interfaces for PSAPs not yet fully transitioned to NG911 CHE. Legacy bridging is implemented in a manner that does not compromise the security or performance of the NG911 core, and all legacy interfaces are subject to the same RBAC, logging, and audit requirements as native NG911 interfaces.

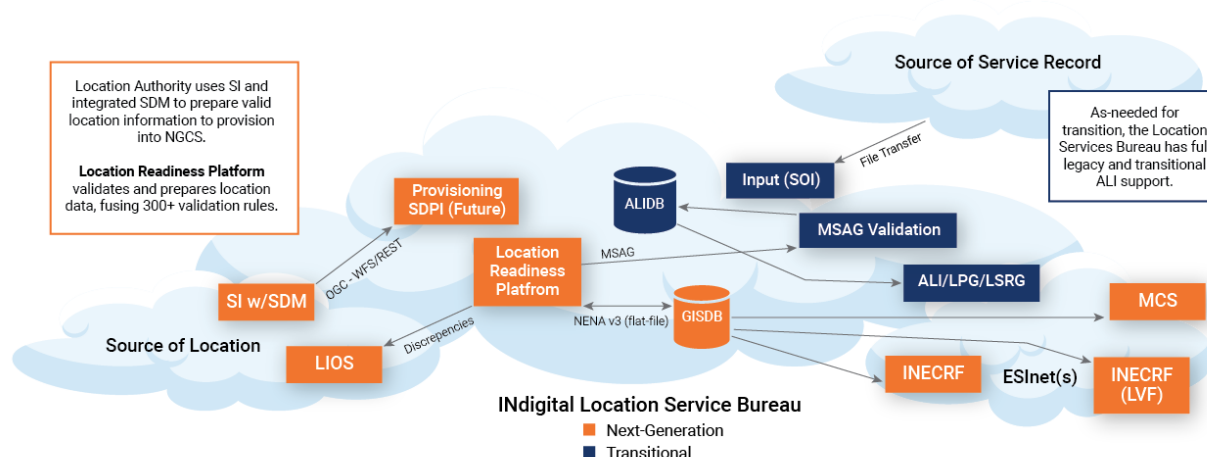
4.2.7 Outgoing Call Interface Function (OCIF) (§E.2.5.1)

INDIGITAL's NGCS supports the Outgoing Call Interface Function (OCIF) as defined in NENA-STA-010.3. The OCIF enables authorized PSAP personnel to initiate outbound calls through the ESInet, including callbacks to 911 callers and inter-agency coordination calls. Outbound calls traverse the same secured SIP infrastructure as inbound emergency calls, with mutual TLS authentication, call logging, and policy enforcement applied to all outgoing sessions. The OCIF integrates with the ESRP and BCF to ensure that outbound routing follows the same security and quality-of-service policies governing inbound call processing.

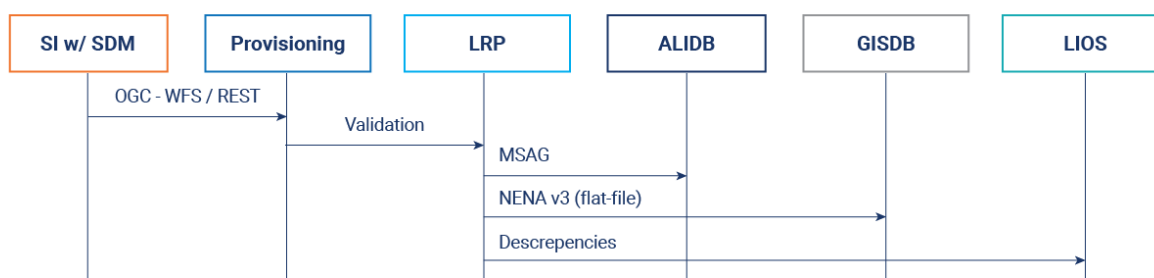
4.3 GIS and Location Technical Narrative (§E.3)

RFP §E.3: 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). Location data shall be transported using PIDF-LO per RFC 4119 and RFC 5139 with applicable NENA extensions. The GIS system shall provide change tracking, version control, time-stamped snapshots, and automated batch or incremental updates using NENA provisioning interfaces.

INDIGITAL fully complies with all requirements set forth in RFP §E.3 GIS and Database Services Requirements. GIS data management is included in the base proposal scope per Addendum 2, Q&A #13 – it is not an optional service. INDIGITAL's GIS architecture is purpose-built for NG911 accuracy and speed, anchored by our Data Integrity Gateway (DIG) and Location Integrity Oversight Service (LIOS), which together deliver the 5-minute routing update SLA that the Nebraska PSC requires.



GIS Data Pipeline



LDB Data Pipeline

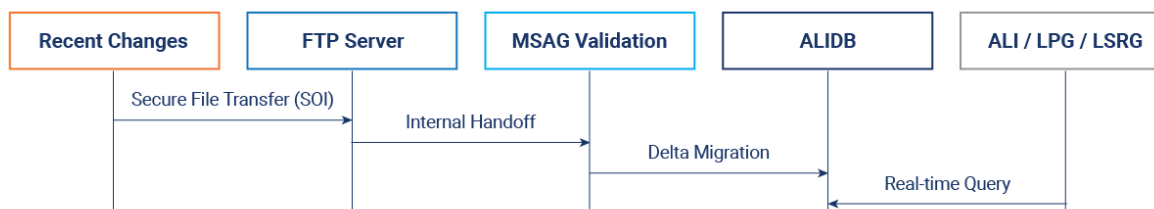


Image 4.3-1 This image shows the data flow through the INDIGITAL data architecture.

4.3.1 Data Management and GIS Foundation (§E.3.1)

4.3.1.1 NENA GIS Data Model Conformance

All GIS data used in Nebraska's NG911 routing is stored, managed, and served in conformance with NENA-STA-006.2-2022. INDIGITAL accepts GIS data submissions from Nebraska's counties and PSAPs in the NENA GIS Data Model schema, normalizes and validates incoming data against NENA schema requirements, and maintains all required NENA layers: PSAP service boundaries, Emergency Service Number (ESN) boundaries, address points, civic addressing, street centerlines, and emergency routing attributes.

The GIS repository uses a spatially indexed database with support for all NENA-required geometry types, enabling efficient spatial queries that meet the sub-second response time requirements for ECRF routing lookups. Spatial indexing is implemented and maintained as part of our standard operating procedures — not as an optional enhancement.

4.3.1.2 Data Integrity Gateway (DIG) & GeoComm Spatial Interface (§3.1.2)

GeoComm's role in the Nebraska engagement is the Spatial Interface — the managed layer through which Nebraska's county GIS authorities submit, validate, and provision authoritative GIS data to INDIGITAL's ECRF and LVF. INDIGITAL retains full prime-contractor accountability for all GIS data quality, routing accuracy, and SLA performance. GeoComm operates under INDIGITAL's direction and within the integrated GIS architecture described in this section. INDIGITAL's Data Integrity Gateway (DIG) serves as the Spatial Interface (SI) between the GIS data management layer and the ECRF/LVF. The DIG validates all incoming GIS data against NENA-STA-006.2 schema requirements, performs geometry validation (topology checks, gap/overlap detection, attribute completeness), and pushes validated data into the ECRF and LVF in near real time.

The 5-minute GIS propagation SLA — required by RFP §E.3 and confirmed in Addendum 2, Q&A #11 as intentional — is the operational commitment of the DIG. The 5-minute window runs from when the authoritative GIS authority releases a change to when the ECRF reflects it; the eight-second window is the final segment — from when the SI presents validated data to the DIG to when it is active in the ECRF.

4.3.1.3 GeoComm GIS Data Hub

GeoComm's core platform is the GIS Data Hub (GDH), a cloud-native GIS data management solution that provides the Spatial Interface, quality control, aggregation, and ECRF/LVF provisioning functions for Nebraska's NG911 deployment. The GDH operates as the single authoritative system through which county GIS data is ingested, validated, merged into a statewide dataset, and provisioned to INDIGITAL's NGCS components. The GDH workflow proceeds through the following stages:

County and PSAP GIS data maintainers submit their locally authoritative datasets to the GIS Data Hub through a secure web interface using a drag-and-drop upload process. The GDH accepts data in each agency's native GIS schema — counties are not required to reform their data for NG911 purposes. GeoComm's ETL process maps local schemas into the Nebraska NG911 data model, deriving fields that agencies do not maintain directly from other available sources where possible. This means agencies keep their existing workflows unchanged.

Submitted data undergoes a comprehensive set of configured quality control checks covering: feature-level attribute validation (field mismatches, duplicate values, missing identifiers); feature-level geometry validation (misaligned polygons, overlaps, overhangs); geometry integrity checks (gaps, null geometry, unnecessarily complex shapes); synchronization checks between GIS fields and MSAG/ALI data; unacceptable value detection per user-specified rules; and projection verification. QC checks are performed at both the individual jurisdiction level and on the statewide aggregated dataset. Only datasets passing all critical error checks are incorporated into the statewide dataset – non-passing datasets are not silently dropped. The submitting agency receives immediate notification and an actionable error report enabling prompt correction and resubmission.

Once validated data is aggregated into the statewide dataset, the GDH provisions the final dataset to INDIGITAL's ECRF and LVF through GeoComm's standards-based Spatial Interface. Provisioning is structured, automated, and near-real-time. The SI converts validated GIS data into the format and projection required by INDIGITAL's ECRF and LVF and pushes updates through structured automated workflows. The combined GeoComm GDH-to-DIG-to-ECRF/LVF pipeline consistently meets the five-minute routing propagation SLA required by the RFP and confirmed in Addendum 2, Q&A #11. Beyond the ECRF and LVF, the GDH also distributes data packages to PSAPs for use in CAD and mapping systems, ensuring consistency across all NG911 data consumers.

As part of every data upload cycle, the GDH performs a comparison between submitted GIS data and the MSAG and ALI database, reporting synchronization results to local authorities. This provides both a continuous quality metric and a practical tool for Nebraska's counties to track their progress toward full GIS-to-MSAG synchronization during the transition period. The GDH also supports generation of a GIS-derived MSAG and GIS-derived MSAG delta file with each quality data submission, supporting Nebraska's transition from legacy MSAG-based routing.

GeoComm's GIS Data Hub provides web-based analytics, reporting, and Esri Dashboard views showing data submission currency by agency, error counts, and synchronization rates. GeoComm will develop and maintain a Nebraska-specific statewide NG911 readiness dashboard in collaboration with the State GIS coordinator and the PSC.

4.3.1.4 Maintain — Operational Definition

Per Addendum 2, Q&A #32, 'maintain' means that INDIGITAL hosts and manages the operational GIS datasets used for NGCS call routing – including all required NENA layers, quality control, and synchronization. Maintenance is not limited to data storage. INDIGITAL's GIS data management services include: operational hosting of all NENA GIS layers; regular quality control audits against NENA-STA-006.2 requirements; synchronization of all layers across ECRF, LVF, and LDB instances; coordination with Nebraska county and PSAP GIS data stewards for update submission and discrepancy resolution; and proactive identification and correction of data quality issues before they impact call routing.

GeoComm's value to this engagement is not theoretical. GeoComm currently maintains the authoritative NG911 GIS data for 82 of Nebraska's 93 counties, which are served by 58 of 68 PSAPs. GeoComm's team of GIS professionals uses the GIS Data Hub internally for all data quality control, aggregation, and provisioning for these Nebraska customers today. All local data maintainers in GeoComm's current Nebraska footprint already use the GIS Data Hub workflow and will continue using the same system and familiar process to submit their data for

NG911 provisioning — eliminating retraining overhead and accelerating the path to a conformant statewide routing dataset. The remaining county datasets that GeoComm does not directly maintain also pass through the GIS Data Hub QC checks before provisioning into the statewide dataset, ensuring consistent quality standards across all 93 counties regardless of local maintainer.

4.3.1.5 Location Integrity Oversight Service (LIOS)

INDIGITAL's Location Integrity Oversight Service (LIOS) provides continuous monitoring of the GIS data pipeline from source submission through ECRF deployment. LIOS alerts the GIS operations team when data updates are pending, when propagation SLA timers are approaching threshold, or when data quality checks fail. LIOS maintains a complete audit trail of every GIS update, including the source, the validation result, the propagation timeline, and the ECRF deployment confirmation.

4.3.1.6 Data Governance and Provisioning

The INDIGITAL GIS system provides change tracking, version control, time-stamped snapshots, and automated batch or incremental updates using NENA provisioning interfaces. Every GIS data change is recorded with a timestamp, the identity of the submitting authority, and the change type. Version control allows rollback to any prior state, enabling recovery from erroneous data submissions without service disruption. Automated batch update processing supports both NENA-defined bulk provisioning interfaces and incremental update APIs for real-time boundary changes.

4.3.2 Location Conveyance (§E.3.1)

All location data within the INDIGITAL NGCS is transported using PIDF-LO (Presence Information Data Format — Location Object) per RFC 4119 and RFC 5139, with all applicable NENA extensions as specified in NENA-STA-010.3. Location is delivered to PSAP Call Handling Equipment (CHE) and mapping clients through both push (SIP headers on inbound call) and pull (LIS query) mechanisms, supporting all NG911 call delivery scenarios.

4.3.3 Core Data Services (§E.3.2)

4.3.3.1 Mapping Data Service (MDS, §E.3.2.1)

INDIGITAL's Mapping Data Service supports all layers defined in NENA-STA-006.2-2022 and all features and images described in NENA-STA-010.3. MDS is available within 18 months of contract execution per RFP §E.3.2.1. The MDS exposes ElementState and ServiceState SUBSCRIBE/NOTIFY interfaces per NENA-STA-010.3, enabling PSAPs and authorized agencies to subscribe to real-time service state updates. The State is able to subscribe to ServiceState and receive all standard state changes through the MDS NOTIFY interface.

Retrieval of map data is controlled by the NENA-STA-010.3 Data Rights Management (DRM) mechanism, ensuring that map data access is governed by agency-level permissions and that unauthorized access is prevented at the service level.

4.3.3.2 MSAG Conversion Service (MCS, §E.3.2.2)

INDIGITAL's MSAG Conversion Service translates between legacy MSAG/ALI address formats and NENA GIS Data Model civic address formats, enabling backward compatibility with legacy selective routers and i3 v2 CHE systems during Nebraska's transition period. MCS supports

bidirectional conversion and maintains synchronization between legacy MSAG records and NENA-format address data.

4.3.3.3 Geocode Conversion Service (GCS, §E.3.2.3)

The Geocode Conversion Service translates street address strings into geographic coordinates and vice versa, supporting location validation, address disambiguation, and ALI data enrichment. The GCS uses the NENA GIS address point layer as its authoritative source, ensuring consistency between geocoded results and the GIS data used for ECRF routing.

4.3.4 PSAP-Facing Services (§E.3.3)

4.3.4.1 PSAP Mapping Service (§E.3.3.1)

INDIGITAL provides a PSAP Mapping Service that delivers real-time map data and call location display to PSAP positions. The mapping service is integrated with the call delivery system, automatically presenting the caller's location on the PSAP dispatcher's map display at call answer. The PSAP Mapping Service does not interfere with or materially change any existing PSAP CHE contract, per RFP §E.3.1 requirements.

4.3.4.2 Map Discrepancy Reporting (§E.3.3.2)

INDIGITAL provides a structured map discrepancy reporting tool allowing PSAP personnel to report GIS data errors – incorrect boundaries, missing address points, or inaccurate routing – directly from the PSAP interface. Discrepancy reports are routed to the INDIGITAL GIS operations team and to the appropriate county or PSAP GIS data steward for review and correction. Each report is tracked through resolution, with the PSAP submitter receiving confirmation when the underlying GIS data has been corrected and propagated.

4.3.5 External GIS Integrations (§E.3.4)

INDIGITAL's GIS platform is designed for open integration with external GIS systems, including Nebraska county GIS departments, state GIS clearinghouses, and any authorized third-party GIS data providers. Integration uses standard APIs aligned to NENA provisioning interfaces, minimizing custom integration work and ensuring that Nebraska's existing GIS investments remain usable within the NG911 architecture.

4.4 Security Technical Narrative (§E.4)

RFP §E.4: The contractor shall implement the NENA NG-SEC security and trust model, featuring strong authentication and authorization for all interfaces, mutual TLS. All location data, call content, and PII must be encrypted in transit (TLS 1.3) and at rest (AES-256 or stronger). The contractor must operate a standards-based PKI to uniquely identify and authenticate every participating agency and agent.

INDIGITAL fully complies with all requirements set forth in RFP §E.4 Security Requirements. Our security architecture is built on the NENA NG-SEC model and implements defense-in-depth across all nine security domains required by NENA-STA-040.2-2024. Nebraska's 911 infrastructure is protected by independently verified security controls – not self-certified claims – and managed by a dedicated security architect with named accountability. INDIGITAL has participated in and supported independent security audits and assessments. The results and reports from these assessments, including penetration testing, are owned by the governing 9-1-

1 entity and the 3rd party auditors. INDIGITAL is willing to work with the Nebraska PSC and NG911 program team to review such reports in a controlled environment.

4.4.1 Security Management and Process Control (§E.4.1)

4.4.1.1 Personnel Roles and Responsibilities (§E.4.1.1)

INDIGITAL defines, assigns, and documents all minimum-security roles and responsibilities required by RFP §E.4.1.1. Named, accountable individuals are assigned to every required security role. Security responsibilities are not distributed across unnamed role pools — every function has a named owner.

INDIGITAL's dedicated Security Architect for Nebraska is **Robert Brown, CIO / CSO**. Robert leads all security architecture, PKI management, incident response, and FIPS compliance activities for this engagement. He provides the organizational RACI matrix identifying security roles, responsibilities, and escalation paths across all nine NENA-STA-040.2 security domains.

4.4.1.2 Personnel Roles and Responsibilities — Required Security Roles Matrix (§E.4.1.1)

Per RFP §E.4.1.1, INDIGITAL defines, assigns, and documents the following minimum-security roles and responsibilities across the Nebraska ESInet and NGCS. All roles are covered by named, accountable individuals. Where shared or combined roles exist, the accountable individual for each responsibility is noted. Third-party assignments are governed by contractual obligations and verified through attestation, SLAs, and right-to-audit provisions.

#	RFP-Named Role	RFP Authority / Scope	Named Individual	Title	Proposal Deliverable Required
1	Security Manager	Authority to set security policy for all NGCS/ESInet components; ultimate accountability for all security roles and responsibilities across the contract term.	Robert Brown	CIO / Chief Security Officer	Org roles matrix / RACI; documented role definition; acknowledgement/training evidence.
2	Security Administrator	Implements and enforces security controls across NGCS applications, ESInet, edge devices, and management portals in accordance with NG911 policies.	Robert Brown	CIO / Chief Security Officer	Security administration procedures; documented role definition; evidence of role assignment.
3	Data Owner(s)	Accountable for every NG911 data set (local and remote); defines classification and handling requirements; entries required in the data ownership register.	Ira Pyles	Sr. Solution Architect	Data ownership register mapping every NG911 data set to a named Data Owner with classification and handling responsibilities.
4	Data Custodian(s)	Manage operational security measures for all NG911 data at rest and in transit: encryption, key management touchpoints, access administration, and backup/restore.	GeoComm	Data Custodian	Data custodianship register mapping every NG911 data set (at rest and in transit) to a named Data Custodian with operational security measures documented.

#	RFP-Named Role	RFP Authority / Scope	Named Individual	Title	Proposal Deliverable Required
5	Data User Populations	Defined user populations (not necessarily individual names) who access NG911 data must be mapped to NGCS components and ESInet segments in the RACI.	GeoComm	N/A	RACI with population definitions mapped to NGCS components and ESInet segments; documented data access controls per population.
6	Security Audit Manager	Governs audit cadence (internal and external), scope, reporting, risk rating of findings, and tracking findings to closure; ensures continuity via documented delegation procedures.	Robert Brown	CIO / Chief Security Officer	Audit governance plan covering periodic cadence, scope, reporting format, risk rating methodology, and closure tracking.

4.4.1.3 Nebraska NG911 ESInet/NGCS — Security Roles RACI Matrix

RFP §E.4.1.1 Required Submission | Solicitation #202691101 | INDIGITAL (Communications Venture Corp)

Per RFP §E.4.1.1: each role must be covered by a named, accountable individual. Shared/combined roles must be noted with the accountable individual identified. Where third parties perform duties, INDIGITAL remains responsible for assignment and verification. This matrix is mapped to NGCS components and ESInet segments as required.

Key:

A/R Accountable and Responsible — single owner who also performs the work **A** Accountable — single owner of the outcome
R Responsible — performs the work **C** Consulted — input required before action **I** Informed — notified after action.

Responsibility / Function	Security Manager	Security Administrator	Data Owner(s)	Data Custodian(s)	Data User Populations	Security Audit Manager
§E.4.1.1 — Personnel Roles & Responsibilities						
Security policy authority — set policy for all NGCS/ESInet	A/R	C	C	C	I	C
Role definition, documentation, and assignment	A/R	R	C	C	I	C
Personnel acknowledgment and training records	A	R	I	I	R	I
Data ownership register (classification and handling)	A	C	R	C	I	C
Data custodianship register (encryption, key mgmt, backup)	A	C	C	R	I	C
Security admin procedures — NGCS, ESInet, edge, portals	A	R	I	C	I	I
Audit governance plan — cadence, scope, reporting, findings	A	C	C	C	I	R
Role coverage and delegation during absence	A	R	I	I	I	I
Third-party / subcontractor role verification	A/R	C	I	I	I	C

Responsibility / Function	Security Manager	Security Administrator	Data Owner(s)	Data Custodian(s)	Data User Populations	Security Audit Manager
§E.4.1.2 – Identity Management / PKI						
PKI/CA architecture and CP/CPS oversight	A	R	C	C	I	C
Certificate lifecycle – issuance, renewal, revocation	A	R	I	C	I	I
FIPS 140-2 key protection enforcement	A	R	I	R	I	C
mTLS enforcement across all NGCS/ESInet interfaces	A	R	I	C	I	I
§E.4.1.2.1 – Role Model and Governance						
Agency/agent role governance and approval	A	R	C	I	C	I
Role lifecycle – assignment, revocation, leaver workflows	A	R	C	I	I	I
Role use monitoring and audit	A	C	I	I	I	R
§E.4.1.3 – Policies and Procedures						
Cybersecurity policy framework – ownership and approval	A/R	C	C	C	I	C
Policy governance – versioning, distribution, review cadence	A	R	I	I	I	C
SOP catalog authorship and maintenance	A	R	C	C	I	C
Vendor / subcontractor policy flow-down enforcement	A	R	I	I	I	C
§E.4.1.3.1 – Incident Response / BC/DR						
CIRP ownership, maintenance, and testing	A	R	C	C	I	C

Responsibility / Function	Security Manager	Security Administrator	Data Owner(s)	Data Custodian(s)	Data User Populations	Security Audit Manager
BC/DR plan ownership and annual testing	A	R	C	C	I	C
Incident detection and triage – SIEM/IDS	A	R	I	I	I	I
External assistance engagement authority	A/R	C	I	I	I	I
§E.4.1.4 – Authorization and Data Rights Management						
XACML policy authoring, signing, and lifecycle	A	R	C	I	I	C
Data rights management – provisioning data ownership	A	C	R	C	I	C
PDP/PEP architecture and decision logging	A	R	I	C	I	C
§E.4.2 – Information System Infrastructure and Management						
Device / software / cloud inventory management	A	R	C	R	I	C
Patch and vulnerability management program	A	R	I	C	I	C
Network segmentation architecture	A	R	I	C	I	I
Boundary protection – BCF/NGFW management	A	R	I	C	I	I
§E.4.3 – Authentication and Federated SSO						
Federated SSO architecture and enforcement	A	R	I	C	I	I
§E.4.4 – Cryptography and Public Key Infrastructure						
HSM / cryptographic module management	A	R	I	R	I	C

Responsibility / Function	Security Manager	Security Administrator	Data Owner(s)	Data Custodian(s)	Data User Populations	Security Audit Manager
Key generation, rotation, and escrow	A	R	I	R	I	C
§E.4.5 – Integrity Protection						
JWS signing for XACML policies	A	R	C	I	I	I
§E.4.6 – Information Privacy						
Privacy controls and data handling	A	C	R	R	C	C
§E.4.7 – Security Assessment and Audit						
Penetration test oversight and remediation tracking	A	R	C	C	I	R
External compliance audit management	A	C	C	C	I	R
Internal audit program	A	C	C	C	I	R
Findings risk rating and closure tracking	A	C	C	C	I	R
§E.4.8 – Security Monitoring, Detection, and Alerting						
SIEM operations and alert response	A	R	I	C	I	I
IDS/IPS management	A	R	I	I	I	I
DoS/TDoS monitoring and response	A	R	I	I	I	I

Notes

1. The Security Manager role holds Accountable (A) on every row per RFP §E.4.1.1, which grants that role authority to set security policy across all NGCS/ESInet components.

2. Data Owner(s) and Data Custodian(s) may each represent multiple individuals mapped by data set. The RFP requires a data ownership register and a data custodianship register identifying every NG911 data set.
3. Where roles are shared or combined, the accountable individual must be identified and noted in the submission per §E.4.1.1.
4. This matrix includes NGCS component and ESInet segment mapping columns as required for submission.
5. Named individuals have been assigned to all six roles. Role assignments confirmed by Robert Brown, CIO/CSO. NGCS component and ESInet segment mapping incorporated per Note 4.

4.4.2 Incident Response Plans (§E.4.1.3.1)

INDIGITAL fully complies with RFP §E.4.1.3.1. We maintain a formal, written Cybersecurity Incident Response Plan (CIRP), a Business Continuity (BC) Plan, and a Disaster Recovery (DR) Plan as separate, complementary documents. Each plan is aligned to NIST SP 800-61 Rev. 2 and the NENA NG-SEC framework, is staffed by trained responders with named accountability, and is tested at least annually through tabletop and live exercises. The following sections describe how INDIGITAL meets each requirement identified in this section.

4.4.2.1 Cybersecurity Incident Response Plan (CIRP)

INDIGITAL maintains a written Cybersecurity Incident Response Plan structured around the four phases required by this section: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity. The CIRP is owned by Robert Brown, CIO/CSO, who serves as the named Security Manager for the Nebraska engagement per §E.4.1.1. The plan is a living document, updated annually and after every significant security event, with version control and formal change tracking maintained through our document management system.

4.4.2.2 Phase 1: Preparation

Preparation is the foundation of effective incident response. INDIGITAL's preparation posture includes the following elements:

Security Team Structure. INDIGITAL's security team consists of the CIO/CSO, a senior security analyst, and a junior security analyst, supported by the VP of Operations and CTO. For the Nebraska engagement, Robert Brown (CIO/CSO) leads all security architecture, PKI management, incident response, and FIPS compliance activities, as documented in the RACI matrix at §4.4.1.

Incident Response Team Structure. INDIGITAL uses a distributed response model to account for the geographic diversity of the Nebraska ESInet and NGCS infrastructure. Each incident response team consists of, at minimum, one security team member, NSOC operations staff, the regulatory/compliance liaison, the local market or area manager, field technicians as needed, network and server team members as applicable, and third-party specialists when warranted. This model ensures that every incident has both centralized security oversight and local operational knowledge at the point of impact.

Defined Roles and Responsibilities. The regulatory liaison and local manager are responsible for coordinating and communicating with the Nebraska PSC, affected PSAPs, and other external stakeholders. The security team member coordinates with INDIGITAL executive management and ensures the necessary internal resources are engaged. All team members are responsible for internal communications, evidence capture, and documentation throughout the incident lifecycle.

Tools and Infrastructure. Preparation includes maintaining the detection and monitoring infrastructure described in §4.4.5, including SIEM, IDS/IPS (Fortinet), third-party Managed Detection and Response (MDR), and 24x7x365 NSOC staffing. All monitoring platforms are kept current, with detection signatures and threat intelligence feeds updated continuously.

Communications Framework. Incident communications use voice (direct and telecommunication), email, Slack, and text messaging. All team members are responsible for tracking their communications and activities against a designated time source to ensure

completeness of after-action reporting. Pre-established notification trees ensure the Nebraska PSC receives notification within contractually defined timeframes for high-severity incidents.

Incident Declaration and Classification Criteria. INDIGITAL defines a security incident as a measurable change in system state accompanied by negative consequences, including but not limited to unauthorized access to systems or data, inability to use systems for their intended purposes, and destruction of data or systems. Events are classified by severity using the following criteria:

- Category 1 (Critical): Complete or partial loss of 911 call delivery, active data breach involving PII or call records, ransomware affecting production systems, or any event requiring immediate PSC notification.
- Category 2 (High): Degraded service affecting call processing performance, unauthorized access attempt that reached an internal system, confirmed malware on any ESInet or NGCS component, or DDoS/TDoS attack exceeding baseline thresholds.
- Category 3 (Medium): Suspicious activity detected by SIEM or IDS that requires investigation, failed login attempts exceeding threshold, unauthorized configuration change detected, or vulnerability scan revealing a critical CVE on a production system.
- Category 4 (Low): Informational security events, policy violations without system impact, phishing attempts blocked by controls, or routine anomalies resolved through standard triage.

4.4.2.3 Phase 2: Detection and Analysis

INDIGITAL employs a layered detection architecture that combines automated tooling with informed personnel to enable early identification of security events.

SIEM Platform. All ESInet and NGCS components generate centralized, immutable audit logs that are aggregated into the SIEM platform for real-time correlation with threat intelligence feeds. The SIEM enables security events across the full attack surface, correlating alerts from firewalls, IDS/IPS, endpoint detection and response (EDR), application logs, and authentication systems. Role-based access controls govern access to audit records, ensuring log data cannot be modified or deleted by unauthorized personnel.

IDS/IPS (Fortinet). The proposed solution uses Fortinet intrusion prevention systems within the ESInet BCF framework. Fortinet IPS provides detection and survivability against zero-day attacks, advanced targeted attacks, ransomware, polymorphic threats, and distributed denial of service (DDoS) attacks. The IPS includes multiple inspection engines, threat intelligence feeds, and advanced threat protection options. IPS operates in inline blocking mode for high-confidence, high-severity detections, automatically dropping malicious traffic before it reaches protected NGCS components. All IPS blocking actions are logged with full packet capture for forensic review.

Third-Party Managed Detection and Response (MDR). Beyond INDIGITAL's own NSOC monitoring, we contract with a third-party MDR vendor that uses layer 2 network monitoring to provide predictive analysis at all data center locations. By actively analyzing data packets entering and leaving the network, the MDR service can identify and isolate threats, including ransomware, before they spread. This capability is independent of the endpoint security solution deployed at each PSAP. The MDR vendor delivers regular in-depth vulnerability reports with remediation recommendations to the INDIGITAL security team and contacts the NSOC directly with any identified concerns requiring immediate action.

Staff Reporting. All INDIGITAL staff are trained to recognize indicators of compromise and to report suspected cyber events to the NSOC. The NSOC can be reached 24x7x365 by email or phone. External stakeholders, business partners, and customers who suspect or witness events that could impact INDIGITAL systems also report through the NSOC. Upon receiving a report, the NSOC opens a support ticket and notifies members of the security team immediately.

Triage Workflows. Detection follows a structured triage process: signs of an incident are classified as either precursors (signs that an incident may occur in the future) or indicators (signs that an incident may have occurred or is occurring now). NSOC analysts baselined expected activity levels through profiling so that deviations from normal patterns are identified quickly. Team members who understand normal behavior through regular review of log entries and security alerts are positioned to recognize abnormal behavior, investigate unusual entries, and escalate to incident status when classification criteria are met.

Severity Classification and Escalation. Detected events are assessed against the classification criteria defined in Phase 1. Events that meet or exceed Category 3 criteria are escalated to the incident response team. Category 1 events trigger immediate notification to the Nebraska PSC, with a defined escalation path that reaches INDIGITAL executive leadership within defined timeframes. The NSOC generates automated alarms for Category 1 and Category 2 events.

4.4.2.4 Phase 3: Containment, Eradication, and Recovery

Once an event has been detected and classified as an incident, the incident response team moves through containment, eradication, and recovery in a disciplined sequence designed to preserve evidence, limit damage, and restore services as rapidly as possible.

Containment. The team determines the best methods to mitigate existing risk and narrows the possibility of further compromise. Containment actions are tailored to the scope and nature of the incident and may include isolating a network segment, applying access control lists, removing or disconnecting affected systems, and diverting traffic to known-good backup systems. For incidents affecting production 911 call delivery, containment prioritizes maintaining call flow continuity. INDIGITAL's active-active data center architecture (described in §4.7) provides immediate failover capability, ensuring that containment actions at one facility do not interrupt call delivery from the other.

Evidence and Data Capture. Documentation begins as soon as the team suspects an incident has occurred. Every step taken from detection through final resolution, is documented and timestamped against a designated authoritative time source. The team captures volatile system evidence where applicable, including lists of network connections, processes, login sessions, open files, network interface configurations, and memory contents. Full forensic disk images are obtained, when possible, as imaging is preferred over performing analysis on original systems to preserve evidence integrity. All evidence handling follows procedures that maintain chain of custody for potential legal proceedings.

Root Cause Analysis. The team pinpoints both current indicators and potential precursors to determine the type, extent, and magnitude of the problem, validates the analysis to rule out false positives, and identifies the scope, points of origin, and attack vectors involved.

Prioritization. When multiple events or incidents occur simultaneously, response and resources are prioritized based on functional impact to 911 call delivery, information impact (sensitivity of data at risk), service level agreement obligations, the size and type of resources affected, and the potential for lateral movement to additional systems.

Eradication. The team identifies the root cause, removes malware or threats, and addresses the vulnerability that enabled the attack. If a weak authentication mechanism was the entry point, it is replaced with strong authentication. If a software vulnerability was exploited, it is patched immediately. Eradication is confirmed through verification scanning before recovery proceeds.

Service Restoration. Affected production systems are brought back online through a controlled process that verifies the threat that has been fully eliminated before restoration. The team evaluates the confidence factor for each restoration method: whether recovery from backup is acceptable or whether the system should be rebuilt from a known-clean baseline. For NG911 production systems, restoration procedures leverage the redundant architecture described in §4.7 to maintain service continuity throughout recovery. The five-second RTO target described in the failover scenarios at §4.9 applies to call delivery restoration.

4.4.2.5 Phase 4: Post-Incident Activity

After-Action Review. As soon as possible, and no later than two weeks from the end of the incident, the team conducts a formal after-action review. The review covers: documentation that could not be prepared during the active response; full investigation of the incident's scope; how containment and eradication were achieved; what was done to recover affected systems; areas where the response was effective; and areas requiring improvement. A complete report is submitted to INDIGITAL senior management and, for incidents affecting Nebraska NG911 services, to the Nebraska PSC.

Lessons Learned. During the after-action review, lessons learned are identified, captured, and reviewed with the team and senior management. Each lesson is assigned a specific action for either improving future response or strengthening preventive controls. Lessons learned feed directly into updates to the CIRP, training curricula, and detection rule sets.

Continuous Improvement. INDIGITAL practices within the ITIL framework for continuous service improvement. This philosophy applies to our cybersecurity posture, our response to incidents, and the CIRP itself. Each incident or exercise generates improvements that are tracked through resolution.

4.4.2.6 Detection Capabilities and Processes

INDIGITAL's detection architecture is described in detail at §4.4.8 (Security Monitoring, Detection, and Alerting). In summary, early detection is enabled through:

- SIEM with centralized log aggregation, real-time correlation against threat intelligence feeds, and automated alerting for anomalous patterns across all ESInet and NGCS components.
- IDS/IPS (Fortinet) providing deep packet inspection, rate limiting, and inline blocking at ESInet boundaries, with detection capabilities for zero-day, ransomware, polymorphic, and DDoS/TDoS threats.
- Third-party MDR provide layer 2 network monitoring, predictive analysis, full packet capture, and forensic data capture at all data center locations.
- NSOC personnel trained to establish baselines for normal operation, set alert thresholds for deviations, and triage events through structured workflows that classify severity and determine whether escalation to incident status is warranted.
- Staff reporting through 24x7x365 NSOC channels, with all employees trained in incident recognition as part of the cybersecurity awareness program.

- DDoS/TDoS-specific detection including traffic baselining and threshold alerting at the BCF, trunk saturation monitoring via LNG and SBC thresholds, source identification using IP address, ANI, and pANI, and STIR/SHAKEN call authentication as described in §4.4.5.2.

4.4.2.7 Training and Exercise Evidence

INDIGITAL maintains a comprehensive training program that ensures all personnel with incident response duties are prepared to execute the CIRP effectively.

Cybersecurity Awareness Training. All INDIGITAL staff are required to complete cybersecurity awareness training upon hire and annually thereafter. The program covers threat recognition, reporting procedures, password hygiene, physical security, and social engineering awareness. Quarterly phishing simulation exercises are conducted to test and reinforce training effectiveness, with additional training assigned to staff who do not meet performance thresholds.

Incident Response Training. Personnel assigned to the incident response team receive role-specific training covering their responsibilities under each CIRP phase. This includes evidence handling and chain-of-custody procedures, forensic imaging techniques, communications protocols, and the use of detection and analysis tools. CJIS training and certification is completed by all staff who require access to criminal justice information.

Documented Improvements. All after-action reviews from both real incidents and exercises generate documented improvement actions. These actions are tracked to completion and incorporated into the next CIRP revision cycle.

4.4.2.8 Business Continuity (BC) Plan

INDIGITAL maintains a separate Business Continuity Plan that addresses the preservation of critical NG911 services during and after any disruption, whether caused by cyberattack, natural disaster, infrastructure failure, or other adverse events. Because 911 must continue answering calls and dispatching responders even under adverse conditions, the BC Plan prioritizes uninterrupted call delivery above all other considerations.

Active-Active Architecture as the BC Foundation. INDIGITAL's BC Plan is built on the active-active, geographically redundant data center architecture described in §4.7. Two in-state Nebraska facilities provide the primary and secondary core, with a geographically distant third facility (more than 100 miles away, outside Nebraska) providing a disaster recovery tier. Every call-path functional element runs simultaneously in at least two locations. Loss of any single facility results in automatic failovers with a target recovery time of five seconds for call delivery, as demonstrated in the failover scenario at §4.9.

Critical Service Continuity. The BC Plan identifies all mission-critical services (call routing, location delivery, PSAP connectivity, logging, and NGCS functional elements) and documents the redundancy and failover mechanisms that protect each one. No PSAP connection relies on a single physical path. Remote PSAPs are connected through their host site with appropriate redundancy for the remote link segment.

PSAP Continuity Coordination. The BC Plan addresses coordination with individual PSAPs to ensure their local contingency plans are aligned with the statewide ESInet continuity posture. When a disruption affects a specific PSAP's connectivity, calls can be rerouted to an alternate PSAP destination or to the MEVO backup system, ensuring no 911 call goes unanswered.

Workforce Continuity. The NSOC operates 24x7x365 with distributed staffing that is not dependent on any single facility. INDIGITAL's distributed response model ensures that incident response, network operations, and customer communications can continue from multiple locations simultaneously.

Supply Chain and Vendor Continuity. The BC Plan addresses critical vendor dependencies, including data center facility operators, IP transport providers, and third-party service partners. Service level agreements with these providers include availability commitments and escalation procedures that feed into the broader continuity framework.

4.4.2.9 Disaster Recovery (DR) Plan

INDIGITAL maintains a separate Disaster Recovery Plan that details the procedures for restoring IT infrastructure and coordinating with ongoing mission-critical operations following a catastrophic event. The DR Plan is designed to work in coordination with the BC Plan: the BC Plan maintains service during the disruption, and the DR Plan restores full operational capacity afterward.

Recovery Tiers. The DR Plan establishes recovery priorities based on service criticality:

- Tier 1 (Immediate, RTO less than 5 seconds): Call delivery, PSAP connectivity, location services. These are maintained through active-active failover and do not require manual DR activation.
- Tier 2 (Short-term, RTO less than 4 hours): NGCS administrative functions, SIEM and logging services, management plane access, monitoring dashboards. These services are restored from the surviving data center or the geographically distant third facility.
- Tier 3 (Medium-term, RTO less than 24 hours): Non-production systems, lab environments, reporting and analytics, archival access.

IT Restoration Procedures. The DR Plan documents step-by-step procedures for restoring each system tier, including: validation of backup integrity before restoration begins; sequenced recovery of dependent services (network first, then authentication, then application services); verification testing at each stage to confirm recovered systems are operating correctly; and controlled reintroduction of restored systems into the production environment.

Coordination with Ongoing Operations. Because Tier 1 services continue operating through the active-active architecture during a DR event, the DR Plan specifically addresses how restoration activities are coordinated to avoid disrupting the surviving production services. Restoration of the failed facility is performed in a controlled, parallel manner, with traffic rebalanced across both data centers only after full validation.

Data Protection and Recovery. System configurations, call records, and operational data are replicated across data center facilities. The DR Plan documents recovery point objectives (RPOs) for each data category and the replication mechanisms that achieve them. Backup integrity is verified on a scheduled basis, and restoration from backup is tested as part of the annual DR exercise.

4.4.2.10 Plan Maintenance and Accessibility Controls

Ownership and Version Control. The CIRP, BC Plan, and DR Plan are each assigned a named owner: Robert Brown, CIO/CSO, is the accountable owner for all three plans for the Nebraska engagement. Each plan carries a version number, revision date, and formal revision history.

Changes follow a documented change control process that includes review by the security team and approval by the plan owner before publication.

Offline Storage and Accessibility. All three plans are stored in both digital and offline formats to ensure they remain accessible to recovery teams even during a cyber event that compromises IT systems. Digital copies are maintained in the INDIGITAL document management system with access restricted to authorized incident response and management personnel. Offline copies (encrypted removable media) are maintained at each data center facility and at INDIGITAL's corporate headquarters, secured in a manner that ensures recovery teams can access them without depending on systems that may be affected by the incident. Distribution lists are maintained and updated whenever personnel assignments change.

Distribution Controls. Plan distribution follows a need-to-know model. All incident response team members receive current copies upon assignment and whenever a revision is published. The Nebraska PSC receives the current version upon contract execution and upon each annual revision, consistent with the State's oversight responsibilities.

4.4.2.11 Review and Test Cadence

Annual Review. The CIRP, BC Plan, and DR Plan are each reviewed and updated at least annually. The annual review verifies that all contact information, roles, procedures, and technical details remain current and aligned with the deployed infrastructure.

Triggers for Interim Updates. In addition to the scheduled annual review, interim plan updates are triggered by: any significant security incident; changes to the Nebraska ESInet or NGCS architecture; addition or removal of data center facilities; changes in key personnel assignments; changes to regulatory or compliance requirements affecting NG911 security; and lessons learned from exercises or real incidents that identify procedural gaps.

Testing. Each plan is tested at least annually through tabletop exercises. If no real incidents have occurred within six months, a tabletop exercise is conducted. Exercises are designed to test realistic threat scenarios including ransomware, DDoS/TDoS, data center facility loss, and combined cyber/physical events. Test results, including findings and improvement actions, are documented and retained.

Documented Results. All test and exercise outcomes are recorded in a formal after-action report that captures: scenario description, participants, chronology, findings, root causes for any deficiencies, assigned corrective actions with owners and deadlines, and confirmation of completion for each action. These reports are available for PSC review upon request.

4.4.2.12 Containment and Recovery Playbooks

INDIGITAL maintains scenario-specific playbooks that translate the CIRP's general framework into actionable, step-by-step standard operating procedures for the most common and highest-impact threat scenarios. Each playbook covers initial containment, eradication, service restoration, and lessons learned.

4.4.2.13 Malware and Ransomware Playbook

Initial Containment: Upon detection of ransomware or malware on any ESInet or NGCS component, the response team immediately determines whether EDR is present on impacted systems and reviews EDR actions; assesses the possibility for lateral movement to connected systems (CPE, core systems, ANI/ALI, GIS/MIS, MEVO servers, and other endpoints); disables

network shares on affected systems to prevent further encryption; and isolates affected network segments through firewall rules or access control list changes. For production systems, the team verifies that backup systems are isolated from the affected environment before any containment action that could trigger a failover.

Eradication: The team identifies the entry vector, removes the malware or ransomware payload, and addresses the underlying vulnerability. Full forensic imaging is performed before eradication to preserve evidence.

Service Restoration: The confidence factor drives the restoration approach. If the team is certain the threat has been fully eradicated, recovery from backup proceeds. If any doubt remains, affected systems are wiped and rebuilt from a known-clean baseline. For PSAP-facing systems, the team ensures continuity plans are activated so that calls are routed to alternate PSAP destinations or the MEVO backup system during restoration.

Lessons Learned: A formal after-action review is completed within two weeks. Findings are incorporated into detection rules, access controls, and the next CIRP revision.

4.4.2.14 Denial of Service (DDoS/TDoS) Playbook

Initial Containment: The NSOC detects the attack through traffic baselining and threshold alerting at the BCF. For DDoS attacks, Fortinet IPS provides deep packet inspection and rate limiting; WANGuard and upstream IP service provider enterprise DDoS protection provide cloud-based intelligence and traffic rerouting. For TDoS attacks targeting PSAP trunk groups, the team identifies the source using IP address, ANI, and pANI analysis. Mitigation options include auto-attendants with alternate instructions, honeypot insertion in the call flow, DTMF response requirements to filter automated calls, alternate number routing, and IVR-based filtering strategies. STIR/SHAKEN call authentication provides an additional layer of TDoS source validation.

Eradication: Once the attack source is identified and blocked, the team monitors for recurrence and adjusts detection thresholds as needed. Upstream providers are notified to implement origin-network filtering where possible.

Service Restoration: Alternate route paths are available for traffic rerouting during volumetric attacks, preserving emergency call traffic and service availability. Once the attack subsides and filtering rules are confirmed effective, normal traffic patterns are restored.

Lessons Learned: Attack signatures, source data, and timing patterns are documented and incorporated into detection baselines and IPS rule sets.

4.4.2.15 Critical Service Outage Playbook

Initial Containment: For non-cyber critical service outages (data center facility failure, power loss, transport circuit failure), the active-active architecture provides automatic failover. The NSOC generates a Category 1 alarm, and the Nebraska PSC is notified within 15 minutes. An incident ticket is opened with the facility operator and with INDIGITAL engineering.

Eradication: The root cause is identified in coordination with the facility operator or transport provider. Repairs proceed in parallel with continued service delivery from the surviving infrastructure.

Service Restoration: Once the failed facility or circuit is restored and validated through testing, call traffic is rebalanced across the full infrastructure. A failover event report is provided to the Nebraska PSC detailing the event timeline, impact assessment, root cause, and corrective actions.

Lessons Learned: Each outage event produces an after-action review that evaluates the failover performance against RTO targets and identifies any architectural or procedural improvements.

4.4.2.16 External Assistance Procedures

INDIGITAL maintains documented procedures for engaging external assistance when an incident exceeds internal response capabilities or when specialized expertise is required.

Criteria for Engaging External Resources. External assistance is engaged when: the incident involves a threat vector or attack methodology outside the expertise of the internal security team; forensic analysis requires capabilities or certifications beyond those available internally; the scope of the incident exceeds the capacity of the internal response team; legal or regulatory requirements mandate independent investigation; or the incident involves potential criminal activity requiring law enforcement coordination.

Required Approvals. The decision to engage external assistance is made by the CIO/CSO (Robert Brown) or, in his absence, the VP of Operations (Steve Lantz). For incidents involving potential legal exposure, INDIGITAL legal counsel is consulted before engaging external parties. The Nebraska PSC is informed whenever external assistance is engaged for incidents affecting Nebraska NG911 services.

Current Resources and Contact Lists. INDIGITAL maintains current contact lists for the following external resources:

- Third-party MDR vendor: Under contract for continuous monitoring and on-call incident response support at all data center locations, providing 24x7x365 cyber operations experts and full packet capture forensic capabilities.
- Independent forensic investigation firms: Pre-identified and vetted for engagement when forensic analysis exceeds MDR vendor scope.
- Law enforcement: Contact procedures for FBI (cyber division), state law enforcement, and NCC Watch for incidents involving critical infrastructure threats.
- IP service providers: Enterprise DDoS protection contacts for upstream mitigation during volumetric attacks.
- Data center facility operators: Emergency contacts and escalation paths for each Nebraska facility and the geographically distant DR facility.
- PSAP contacts: Current notification lists for all 68 Nebraska PSAPs for incident communications.

Contact lists are reviewed quarterly and updated whenever personnel or provider changes occur.

4.4.3 Authorization and Data Rights Management (§E.4.1.4)

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. Policy naming conventions & registries usage. Action model defining Read, Create,

Update, Delete, Execute. Example XACML policy sets. JWS packaging & validation. Data rights management procedures. Policy lifecycle controls. Logging & auditability. Performance & availability targets.

4.4.3.1 Authorization Architecture

INDIGITAL's authorization framework follows the OASIS XACML 2.0 reference architecture, implementing four core components that govern access to all NGCS/ESInet interfaces and protected data paths:

Policy Administration Point (PAP). The PAP is the authoring and management interface where security administrators create, review, and publish XACML policies. The PAP is accessible only to authorized personnel through the management plane, protected by mutual TLS and multi-factor authentication. All policy authoring actions are logged. The PAP maintains the master policy repository with full version history. NENA's i3 PolicyStore is the PAP in the INDIGITAL authorization framework.

Policy Decision Point (PDP). The PDP evaluates access requests against the active policy set based on the i3 PolicyType, and returns permit, deny, or indeterminate decisions. PDPs are deployed at each data center facility as part of the INDIGITAL Data Rights Gateway via PolicyStore, ensuring that authorization decisions are made locally to minimize latency on call-path operations. PDP instances are deployed redundantly across the active-active architecture so that the loss of any single PDP does not interrupt authorization services. Each NGCS functional element that processes protected data (ESRP, ECRF, LVF, Logging Service, BCF) invokes the PDP before granting access to protected resources.

Policy Enforcement Point (PEP). PEPs are embedded at every NGCS/ESInet interface where access control decisions must be enforced using identities trusted from TLS mutual authentication. The PEP intercepts incoming requests, constructs an XACML authorization request containing the subject attributes (authenticated identity, role, agency), resource attributes (data type, classification, owning agency), action (Read, Create, Update, Delete, Execute), and environment attributes (date, time, source network), and forwards the request to the PDP. The PEP enforces the PDP's decision before allowing or blocking the operation. PEPs are present at: all BCF external interfaces; all NGCS functional element APIs (BCF, ESRP, ECRF/LVF, Logging Service); all management plane interfaces; and all inter-agency data exchange paths interacting with NGCS FEs.

Policy Information Point (PIP). The PIP provides additional attribute data to the PDP during policy evaluation. PIPs connect to the identity management system (§4.4.2) for subject attributes, the device inventory (§4.4.3) for resource classification, and the agency registry for agency-level permissions. PIPs are queried by the PDP in real time during policy evaluation when the authorization request does not contain all attributes needed for a decision.

PDP Placement on NGCS/ESInet Interfaces. The Data Rights Gateway, which hosts the PDP, is positioned in line on all protected data paths:

- ESInet boundary (BCF): PEP at the BCF invokes the PDP for all inbound requests from external networks (OSP interconnects, adjacent ESInets, PSAP connections) before forwarding traffic to internal NGCS elements.
- NGCS functional elements: Each functional element (ESRP, ECRF, LVF, Logging Service) includes an embedded PEP that invokes the PDP before processing any data access

request. This ensures that even authenticated, internal-to-internal requests are authorized against the active policy set.

- Management plane: All administrative access to NGCS components, User Interfaces, and APIs pass through a PEP that invokes the PDP, enforcing RBAC policies and ensuring that administrative actions are authorized and logged.
-

4.4.3.2 Policy Naming Conventions and Registry Usage

INDIGITAL's policy naming conventions follow NENA-STA-010.3 §10.30 and §10.33 requirements, ensuring that every policy is uniquely identifiable and traceable to the interface or data structure it governs.

Interface Policy Names. Interface policies are named using the ServiceID~keyword convention defined in NENA-STA-010.3 §10.30, where ServiceID identifies the NGCS functional element and the keyword identifies the specific interface. Examples:

- [LoST~ecrf.state.ne.us](#) (ECRF query interface for Nebraska)
- [ESRP~routing.state.ne.us](#) (ESRP routing decision interface)
- [LIS~location.state.ne.us](#) (LIS location retrieval interface)
- [ADR~retrieval.state.ne.us](#) (ADR data retrieval interface)
- [MDS~notify.state.ne.us](#) (MDS notification interface)

Data Item Names. Data item policies use dot notation derived from OpenAPI JSON object names and optional element tags, per NENA-STA-010.3 conventions. Examples:

- civicAddr.A1 (state-level civic address component)
- civicAddr.A3 (city-level civic address component)
- pidflo.location.geodetic (PIDF-LO geodetic location element)
- eido.AgencyDataComponent.AgencyName (EIDO agency data element)
- callRecord.ANI (call record automatic number identification)
- callRecord.location.civic (call record civic address)

Policy Type Registry. All policies are registered in the Policy Type Registry per NENA-STA-010.3 §10.33. The registry maps each policy to its type (interface access control, data item access control, administrative action control), its own authority (Nebraska PSC, INDIGITAL, or delegated agency), and its current version. The registry is maintained in the PAP and is the authoritative source for all active policy references.

4.4.3.3 Action Model

INDIGITAL's XACML implementation defines five actions that apply to all NGCS interfaces and data structures, consistent with the NENA-STA-010.3 data rights framework:

Read. Retrieve or query data without modification. Applies to: ECRF/LVF location queries, LIS location retrieval, ADR data retrieval, call record access, log data queries, MDS data retrieval, configuration reporting. Example: A PSAP dispatcher queries the LIS for a caller's location. The PEP constructs an XACML request with action=Read, subject=dispatcher identity, resource=pidflo.location, and forwards to the PDP for evaluation.

Create. Generate new data records or objects. Applies to provisioning new civic address records in the LIS, creating new agency entries in the ECRF, submitting new GIS data through the SI, and opening incident records. Example: A GIS administrator provides a new address range in the

LIS. The PEP constructs an XACML request with action=Create, subject=GIS admin identity, resource=civicAddr, and the PDP evaluates against the provisioning policy.

Update. Modify existing data records or configuration. Applies to updating location records, modifying routing rules, changing PSAP boundary definitions, updating agency configurations. Example: The Nebraska PSC updates a PSAP service boundary in the ECRF. The PEP verifies the PSC administrator's authorization to modify ECRF routing data for the specified jurisdiction.

Delete. Remove data records or decommission objects. Applies to removing decommissioned address records, deleting expired provisioning data, purging aged log records per retention policy. Example: An authorized administrator removes a decommissioned address range. The PDP evaluates the deleted action against the data ownership policy and the administrator's role.

Execute. Invoke an operational function or trigger a process. Applies to initiating call routing decisions at the ESRP, triggering failover operations, executing maintenance commands, running diagnostic tests. Example: An NSOC operator initiates a manual failover test. The PEP constructs an XACML request with action=Execute, subject=NSOC operator identity, resource=failover function, and the PDP evaluates against the operational action policy.

4.4.3.4 Example XACML Policy Sets

The following example policy sets demonstrate how INDIGITAL's authorization framework applies permit and deny rules with explicit defaults and attribute conditions.

Example 1: Interface Policy Set, ECRF Location Query ([LoST~ecrf.state.ne.us](https://lo.st.ecrf.state.ne.us))

This policy governs access to the ECRF location resolution interface.

- Permit Rule 1 (PSAP Dispatcher Query): Permit when Subject.Role = "dispatcher" AND Subject.AgencyFQDN is in the list of authorized Nebraska PSAPs AND Resource = "[LoST~ecrf.state.ne.us](https://lo.st.ecrf.state.ne.us)" AND Action = "Read" AND Environment.Time is within the subject's authorized shift window.
- Permit Rule 2 (System-to-System ESRP Query): Permit when Subject.Identity is a valid NGCS functional element certificate AND Subject.Role = "ngcs-element" AND Resource = "[LoST~ecrf.state.ne.us](https://lo.st.ecrf.state.ne.us)" AND Action = "Read" (no time restriction for system-to-system queries).
- Deny Rule 1 (Unauthorized Agency): Deny when Subject.AgencyFQDN is NOT in the authorized agency registry for Nebraska ECRF access.
- Deny Rule 2 (Prohibited Action): Deny when Action = "Delete" OR Action = "Update" (ECRF data modification requires a separate provisioning policy, not the query interface policy).
- Default Rule: Deny. Any request that does not match an explicit permit rule is denied. The PDP returns a denying decision, and the PEP blocks the request. The denying decision is logged with full request attributes for audit review.

Example 2: Data Structure Policy Set, Call Record Access ([callRecord](#))

This policy sets governs access to call record data stored in the Logging Service.

- Permit Rule 1 (Authorized PSAP Supervisor): Permit when Subject.Role = "psap-supervisor" AND Subject.AgencyFQDN matches the PSAP that handled the call AND Resource = "callRecord.*" AND Action = "Read" AND Environment.Date is within the retention period.

- Permit Rule 2 (PSC Audit Access): Permit when Subject.Role = "psc-auditor" AND Subject.AgencyFQDN = "psc.state.ne.us" AND Resource = "callRecord.*" AND Action = "Read" (PSC auditors may access call records from any PSAP for oversight purposes).
- Permit Rule 3 (System Logging): Permit when Subject.Identity is the Logging Service system certificate AND Action = "Create" AND Resource = "callRecord.*" (the Logging Service is authorized to create new call records).
- Deny Rule 1 (Cross-Agency Restriction): Deny when Subject.Role = "dispatcher" AND Subject.AgencyFQDN does NOT match the PSAP that handled the call AND Action = "Read" (dispatchers may only access call records from their own PSAP unless a mutual aid policy exception applies).
- Deny Rule 2 (Modification Prohibition): Deny when Action = "Update" OR Action = "Delete" for any subject (call records are immutable once created; no role is permitted to modify or delete them).
- Default Rule: Deny. Any request not matching an explicit permit rule is denied and logged.

4.4.3.5 JWS Packaging and Validation

All XACML policy objects are packaged and distributed using JSON Web Signature (JWS) per RFC 7515 and the JOSE framework, ensuring integrity and non-repudiation throughout the policy lifecycle.

Policy Signing. When a policy is published from the PAP, the policy owner (or the authorized delegate) signs the serialized XACML policy using their X.509 private key. The JWS header includes the signing algorithm (RS256 or ES256), the certificate chain (included by reference via the x5u header parameter pointing to the certificate URL, or by value via the x5c header parameter when offline validation is required), and the key identifier (kid) for key rotation tracking. The signed JWS object is the canonical form of the policy and is the only form accepted by the PDP.

Certificate and Chain Inclusion. For policy distribution within the ESInet (where the PKI infrastructure is online and accessible), certificates are included by reference using the x5u header parameter. This minimizes payload size and ensures the PDP always validates against the current certificate. For offline or disaster recovery scenarios, the full certificate chain is included by value using the x5c parameter, ensuring that recovery teams can validate policies without depending on online PKI services.

PEP/PDP Signature Validation. Before applying any policy, the PDP validates the JWS signature by: (1) extracting the certificate from the x5u or x5c header; (2) validating the certificate chain against the trusted CA root per the PKI CP/CPS described in §4.4.2; (3) checking certificate revocation status via CRL (Certificate Revocation List) distribution point or OCSP (Online Certificate Status Protocol) responder, with OCSP preferred for real-time validation; and (4) verifying the JWS signature using the validated public key. If any validation step fails, the policy is rejected and an alert is generated to the NSOC.

Key Rotation and Revocation. Policy signing keys follow the same lifecycle as all PKI certificates described in §4.4.2. Key rotation is performed on a scheduled basis (annually) and whenever a key compromise is suspected. When a signing key is rotated, previously signed policies remain valid until their next scheduled review cycle, at which point they are re-signed with the new key. If a key is revoked due to compromise, all policies signed by that key are immediately flagged

for re-signing, and the PDP rejects any policy bearing the revoked key's signature. CRL and OCSP updates propagate within the timeframes defined in the PKI CP/CPS.

4.4.3.6 Data Rights Management Procedures

Data Ownership. All provisioning data within the Nebraska NG911 system has a clearly defined owner. The Nebraska PSC owns statewide routing data, PSAP boundary definitions, and system-level configuration. Individual PSAPs own their local configuration data, call records generated at their facility, and agency-specific provisioning (e.g., local supplementary data). INDIGITAL, as the system operator, is the data custodian for all data and is responsible for enforcing the data owner's access policies but does not own customer data. Data ownership is documented in the data ownership register maintained per §4.4.1.

Ownership Enforcement in Policy. Data ownership is enforced through XACML policies that bind each data object to its own authority. The Subject.AgencyFQDN attribute in every access request is matched against the ownership attribute of the requested resource. Policies ensure that: data owners have full Read access to their own data; data owners can delegate access to other agencies through explicit policy grants administered via the PAP; INDIGITAL operations personnel have the minimum access necessary to perform system administration, with all administrative access logged and auditable; and the Nebraska PSC retains oversight access to all data for regulatory and compliance purposes.

Consent Logging. Every access to sensitive data (PII, call records, location data) generates a consent log entry recording the requested identity, the data accessed, the authorization decision, and the timestamp. Consent logs are retained for the full contract term and are available to the PSC for compliance review.

4.4.3.7 Policy Lifecycle Controls

INDIGITAL's policy lifecycle follows a controlled, auditable process from authoring through retirement:

Authoring. New policies are drafted in the PAP by authorized policy authors (Security Manager or designated delegate). Policy authoring follows a template that requires policy name per the naming convention; target interface or data structure; applicable rules with explicit attribute conditions; a default deny rule; and an effective date.

Peer Review. All new or modified policies undergo peer review by at least one additional authorized policy administrator before publication. The reviewer verifies that the policy correctly implements the intended access control, does not conflict with existing policies, and includes appropriate deny rules and a default deny.

Change Management. Policy changes follow the same change management process described in Vol 3, including documentation of the change rationale, impact assessment, and rollback plan. Policy changes affecting call-path operations require approval through the Change Advisory Board (CAB) with Nebraska PSC representation.

Pre-Production Testing. New and modified policies are evaluated in the non-production lab environment before deployment. Testing verifies that permit and deny rules produce the expected decisions for a representative set of access requests, and that no unintended access is granted or blocked.

Promotion. After successful testing and peer review, policies are promoted to production through the PAP's publication workflow. The policy is signed (JWS) and distributed to all PDP instances. PDP instances reload the policy set and begin enforcing the new policy within the configured refresh interval.

Versioning. Every policy carries a version number that is incremented with each change. The PAP retains the full version history for all policies, enabling audit of any policy state at any point in time.

Rollback. If a published policy produces unintended effects, the previous version can be restored from the PAP's version history and re-signed for immediate deployment. Rollback procedures are documented and tested as part of the policy lifecycle.

Archival. Superseded policies are retained in the PAP archive for the contract term, supporting audit and compliance review. Archived policies retain their JWS signatures for integrity verification.

Signing Authorization. Only the Security Manager (Robert Brown, CIO/CSO) and designated delegates are authorized to sign and publish policies. The signing authority is documented in the RACI matrix at §4.4.1.

4.4.3.8 Logging and Auditability

PEP/PDP Decision Logs. Every authorization decision (permit, deny, indeterminate) at every PEP/PDP is logged with the full XACML request (subject, resource, action, environment attributes); the decision rendered; the policy that produced the decision; and the timestamp synchronized to the authoritative time source per §4.4.5.1. Decision logs are forwarded to the centralized SIEM platform described in §4.4.5 for real-time correlation and alerting.

Retention. Authorization decision logs are retained for the full contract term consistent with the logging retention requirements in §4.8.2 (Logging Service). Logs are stored with encryption at rest and tamper-evident controls to prevent unauthorized modification.

Denied and Exception Event Review. All deny decisions and indeterminate outcomes are flagged for review by the security operations team. Patterns of denied access (e.g., repeated denied requests from a single identity) trigger automated alerts in the SIEM. A weekly review of deny-event trends is conducted by the security team to identify potential policy errors, unauthorized access attempts, or misconfigured client systems. Findings from deny-event reviews feed into the policy lifecycle for corrective action.

4.4.3.9 Performance and Availability Targets

PDP Availability. PDP instances are deployed redundantly across the active-active data center architecture within each FE. The PDP availability target matches the overall system availability target of 99.999% due to distribution. Loss of a PDP instance within any FE at one data center is handled by automatic failover of function to the replacement FE and PDP at the surviving facility, with no interruption to authorization services.

PDP Latency. Authorization decisions are rendered within 10 milliseconds for cached policy evaluations and within 50 milliseconds for evaluations requiring PIP attribute lookups. These targets ensure that authorization overhead does not measurably impact call processing latency or functional element response times.

Decision and Policy Caching. PDP instances cache recently evaluated decisions and frequently accessed policy sets to minimize evaluation latency. Cache entries carry a configurable time-to-live (TTL) that balances performance against policy freshness. Default TTL for decision cache entries is 60 seconds. Default TTL for policy cache entries is 300 seconds. Cache invalidation is triggered immediately when a policy is updated through the PAP, ensuring that new or modified policies take effect within the configured PDP refresh interval regardless of TTL.

Fail-Secure Behavior. If the FE's PDP is unavailable or if policy validation fails (e.g., JWS signature validation failure, expired certificate), the system defaults to deny. No access is granted without a valid, affirmative PDP decision. This fail-secure posture ensures that a PDP outage or policy corruption does not result in unauthorized access to protected resources. For call-path critical operations where a PDP outage could impact 911 call delivery, a local failover cache of the most recent validated policy set is maintained at each PEP, enabling continued authorization decisions using the last-known-good policies until PDP service is restored. The use of cached policies during PDP unavailability is logged as an exception event and triggers an immediate NSOC alert.

4.4.4 Identity Management and PKI (§E.4.1.2)

INDIGITAL operates a standards-based Public Key Infrastructure (PKI) that uniquely identifies and authenticates every participating agency, agent, and system element across the Nebraska ESInet and NGCS.

- Each agency's identity is a globally unique Fully Qualified Domain Name (FQDN) – for example, douglas.psap.ne.us – encoded in the X.509 SubjectAltName (SAN) of the agency's certificate.
- Each agent's identity uses the user@agencyfqdn format – for example, dispatcher1@douglas.psap.ne.us – encoded in the SAN of the agent certificate.
- The Certificate Authority operates under a formal Certificate Policy / Certification Practice Statement (CP/CPS) with documented identity proofing and issuance controls. Agencies that cannot meet those controls use a managed CA that enforces the CP/CPS.
- Automated alerts for expiring certificates are implemented and monitored by the NOC, ensuring that no certificate expires silently and causes a service disruption.

INDIGITAL's NG911 security architecture for the State of Nebraska leverages Amazon Web Services (AWS) CloudHSM to provide a highly secure, scalable, and standards-compliant cryptographic key management solution. AWS CloudHSM delivers FIPS 140-2 Level 3 validated Hardware Security Modules, enabling the generation, storage, and lifecycle management of all private keys and certificates supporting NGCS and ESInet operations within a dedicated, customer-controlled HSM cluster. This architecture ensures that all cryptographic material remains isolated within tamper-resistant hardware, with exclusive key ownership maintained by INDIGITAL and no third-party access to plaintext key material.

Aligned with NENA-STA-040.2 and NIST SP 800-53 guidance, INDIGITAL integrates AWS CloudHSM into its certificate management framework to support mutual TLS authentication, secure SIP signaling, and STIR/SHAKEN identity services. All root and leaf certificates issued under the NIOC trust framework are generated and protected within the HSM boundary, ensuring compliance with NG911 security requirements and industry's best practices. Key lifecycle management includes generation, activation, rotation, backup, and secure

destruction—is enforced through strict role-based access controls, multi-factor authentication, and audited operational procedures.

The AWS CloudHSM deployment is architected for high availability across multiple availability zones, eliminating single points of failure and ensuring continuous cryptographic operations in support of mission critical 911 services. INDIGITAL's Network Operations Center (NOC) continuously monitors HSM health, capacity, and certificate expiration thresholds, initiating proactive renewal and maintenance workflows to prevent service disruption. Comprehensive audit logging of all cryptographic and administrative activities is maintained and made available to the State upon request, ensuring full transparency and compliance.

By combining AWS CloudHSM's hardened infrastructure with INDIGITAL's operational expertise and adherence to NIOC governance, the proposed solution delivers a secure, resilient, and fully compliant key management platform capable of supporting the long-term evolution of NG911 services for the State of Nebraska.

HSM usage aligns with Addendum 2, Q&A #33 guidance: Hardware Security Modules are used for all Certificate Authority (CA) and root key material. Endpoint TLS keys for servers and appliances reside in industry-standard cryptographic modules that meet FIPS 140-3 requirements; note FIPS 140-3 supersedes and is backward-compatible with the FIPS 140-2 modules specified in RFP §E.4.1.2, and that all modules proposed are validated under the current NIST CMVP framework.

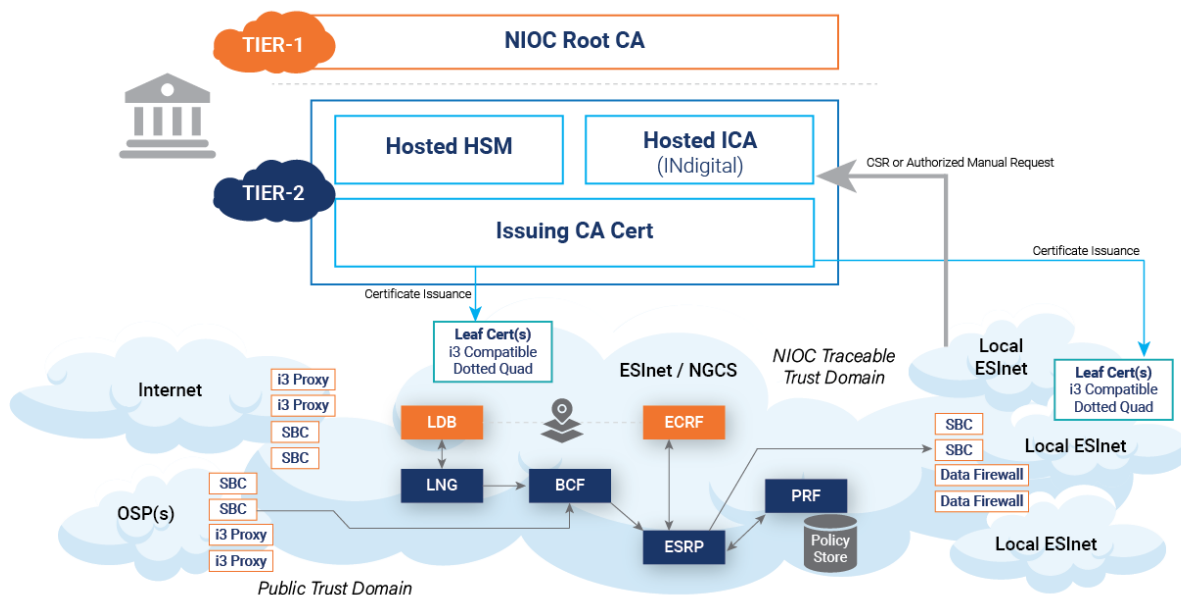


Figure 4.4-1: NIOC Certificate Trust Architecture

This diagram illustrates INDIGITAL's two-tier PKI trust hierarchy for the Nebraska ESNet. At Tier 1, the NIOC Root Certificate Authority establishes the root of trust. At Tier 2, INDIGITAL operates a Hosted Intermediate Certificate Authority (ICA) with a Hosted HSM, which issues an Issuing CA Certificate. Leaf certificates, i3-compatible in dotted quad format, are issued to all ESNet/NGCS elements including i3 Proxies, SBCs, LDB, LNG, BCF, ECRF, ESRP, PRF, and Policy Store components. The architecture defines two trust domains: the Public Trust Domain

(Internet-facing OSP connections) and the NIOC Traceable Trust Domain (ESInet/NGCS internal). Local ESInets receive their own leaf certificates through CSR or authorized manual requests, with data firewalls at local ESInet boundaries. This architecture ensures that every element participating in Nebraska's NG911 network is cryptographically authenticated and traceable to the NIOC root.

4.4.4.1 Federated SSO and External Identity Providers (§E.4.3)

INDIGITAL's NGCS integrates with external identity providers using SAML 2.0 and OAuth 2.0/OIDC, enabling federated single sign-on for PSAP administrators and authorized state agency users. Integration with Nebraska's state identity infrastructure can be configured post-award based on the State's preferred IdP platform.

4.4.5 Information System Infrastructure and Management (§E.4.2)

4.4.5.1 Device Inventory (§E.4.2.1)

INDIGITAL maintains a complete, current inventory of all hardware and software components within the Nebraska ESInet and NGCS. The device inventory is maintained in the configuration management database and is accessible to the PSC at any time. All inventory items are assigned a named owner and a security classification.

4.4.5.2 Patching and Update Management (§E.4.2.2)

INDIGITAL applies security patches on a defined schedule: critical patches within 30 days of release, high patches within 60 days, and medium patches within 90 days. All patches are tested in a staging environment before application to production. Patch application is coordinated with Nebraska PSC through the change management process and never applied *during restricted maintenance periods*.

4.4.5.3 Network Segmentation and Traffic Separation (§E.4.2.3)

All emergency services traffic is logically and physically separated from non-emergency traffic through VLANs, dedicated routing instances, and firewall enforcement at every boundary. Inter-component traffic within the NGCS travels over encrypted, mutually authenticated connections that cannot be intercepted or modified by non-authorized elements on the same physical infrastructure.

4.4.5.4 Network Boundary Protection (§E.4.2.4)

INDIGITAL's boundary protection architecture includes BCFs at all external interconnect points, stateful inspection firewalls at all network segment boundaries, and a layered defense architecture that implements: Demilitarized Zones (DMZ) for all external-facing interfaces (§E.4.2.4.2); defense-in-depth with multiple security control layers between the public internet and any ESInet/NGCS component (§E.4.2.4.3); and strict remote access controls using VPN with multi-factor authentication and session logging for all administrative remote access (§E.4.2.4.4).

All external connections are individually authorized and documented. Unauthorized external connections are blocked at the firewall and alerted in the Security Operations Center (SOC) immediately.

4.4.6 Cryptography (§E.4.4)

All cryptographic implementations in the INDIGITAL NGCS use FIPS-validated modules where the RFP requires FIPS validation, per Addendum 2, Q&A #34. FIPS 140-3 validated modules are used for CA and root key material in HSMS. Endpoint TLS modules meet FIPS 140-2 requirements as FIPS 140-3 is backwards compatible. Where FIPS validation is not explicitly required by the RFP, INDIGITAL still uses industry-standard, well-vetted cryptographic implementations.

- All data in transit is encrypted using TLS 1.3. TLS 1.2 may be supported as a backward compatibility option for legacy endpoints, but TLS 1.0 and 1.1 are disabled on all NGCS interfaces.
- All data at rest – including call records, location data, configuration data, and logs – is encrypted using AES-256 or stronger.
- Data minimization and pseudonymization are applied to all PII in log records and exported data, per applicable state and federal privacy requirements.
- Cryptographic key lifecycle management – key generation, distribution, rotation, revocation, and destruction – is documented in the PKI CP/CPS and enforced through automated key management tooling.

4.4.7 Integrity Protection (§E.4.5)

INDIGITAL fully complies with RFP §E.4.5 Integrity Protection. All data in transit across the ESInet and NGCS is protected against unauthorized modification through TLS mutual authentication and SRTP media encryption as described in §4.4.4 above. Integrity verification is enforced at every inter-component interface using the cryptographic mechanisms described in this section.

4.4.7.1 JSON Web Signatures (§E.4.5.1)

INDIGITAL fully complies with RFP §E.4.5.1 JSON Web Signatures. Policy objects, authorization tokens, and security assertions exchanged between NGCS functional elements are signed using JSON Web Signature (JWS) per RFC 7515 and the JOSE (JSON Object Signing and Encryption) framework. JWS signing ensures that policy content cannot be tampered with in transit and provides non-repudiation for security-critical decisions. The XACML-based Data Rights Gateway described in §4.4.1 enforces JWS validation on all inbound policy objects before they are applied to access control decisions.

4.4.8 Security Monitoring, Detection, and Alerting (§E.4.8)

INDIGITAL fully complies with RFP §E.4.8 Security Monitoring, Detection, and Alerting. Our security operations framework provides continuous monitoring, centralized event correlation, and automated alerting across all ESInet and NGCS components. INDIGITAL operates a 24x7x365 National Service Operations Center (NSOC) with dedicated cyber operations staff providing real-time threat detection and response.

4.4.8.1 Security Event Logging and Continuous Monitoring (§E.4.8.1)

INDIGITAL fully complies with RFP §E.4.8.1 Security Event Logging and Continuous Monitoring. All ESInet and NGCS components generate centralized, immutable audit logs that are collected, correlated, and retained per CJIS Security Policy requirements. Log data is aggregated into the

SIEM platform for real-time correlation with threat intelligence feeds, enabling detection of security events across the full attack surface. Role-based access controls govern access to audit records, ensuring that log data cannot be modified or deleted by unauthorized personnel. A third-party Managed Detection and Response (MDR) vendor provides additional monitoring on administrative and ESInet networks at data center locations, delivering in-depth vulnerability reports with remediation recommendations to the INDIGITAL security team.

4.4.8.2 Time Synchronization (§E.4.8.1.1)

All ESInet and NGCS nodes synchronize to authoritative time sources using NTP per RFC 5905, as described in §4.1.4. Time accuracy is maintained to within plus or minus 10 milliseconds across all network elements, ensuring consistent timestamping for security event logs, call records, and forensic analysis across all Nebraska regions.

4.4.8.3 Denial of Service and Telephony Denial of Service Mitigation (§E.4.8.2)

INDIGITAL fully complies with RFP §E.4.8.2 Denial of Service and Telephony Denial of Service mitigation. Our security architecture addresses all DoS threat categories: volumetric DDoS, application-layer DoS, and Telephony Denial of Service (TDoS) including SIP flooding, spoofing, and injection attacks.

- 4.4.8.3.1 DDoS Detection and Mitigation
 - Detection begins with traffic baselining and threshold alerting at the BCF and network boundary.
 - Fortinet IDS/IPS provides deep packet inspection and rate limiting for anomalous traffic patterns.
 - WANGuard provides additional DDoS detection and mitigation capability with cloud-based intelligence from contracted IP service providers.
 - Alternate routing paths are available for traffic rerouting during volumetric attacks, preserving emergency call traffic and service availability.
- 4.4.8.3.2 TDoS Mitigation
 - TDoS attacks targeting PSAP trunk groups are detected through source identification using IP address, ANI, and pANI.
 - Mitigation capabilities include auto attendants with alternate instructions, honeypot insertion in the call flow, DTMF response requirements to filter automated calls, alternate number routing, and IVR-based strategies.
 - STIR/SHAKEN implementation provides detection of spoofed caller identity, enabling filtering of calls with failed attestation.
 - Behavioral analytics within the Security Operations Center identify abnormal call patterns, SIP message sequences, and registration activity that may indicate TDoS or SIP flooding attacks, enabling automated mitigation before call processing is impacted.

4.4.9 Neb. Rev. Stat. §86-125 Compliance

INDIGITAL does not use any communications equipment that is prohibited under Neb. Rev. Stat. §86-125. The required affidavit confirming this is submitted as a compliance document with this proposal (see Volume 6, Compliance Documents). Our procurement and supply chain management processes include a review of all proposed equipment against the prohibited equipment list prior to any procurement decision.

4.4.10 Information Privacy (§E.4.6)

INDIGITAL fully complies with RFP §E.4.6 Information Privacy. Protecting the privacy of callers, telecommunicators, and all individuals whose data traverses the NG911 system is foundational to our security architecture per NENA-STA-040 Section 6.22 and NENA-STA-010.3 Sections 5.8 and 5.9.

Data Classification and Handling. All data processed by the Nebraska ESInet and NGCS is classified according to sensitivity, with handling rules that govern encryption requirements, access controls, retention periods, and destruction procedures. Classifications align with NENA-STA-040 Section 6.22 requirements for data confidentiality and with NENA-STA-010.3 Sections 5.8 and 5.9 requirements for privacy of location and call content. Data minimization principles are applied so that only the minimum data necessary for each function is exposed, reducing the attack surface for privacy breaches.

4.4.10.1 Access Controls for Sensitive Data

Access to PII, including ANI, ALI, location objects, and multimedia attachments, is governed by the XACML-based Data Rights Gateway described in §4.4.1. Every access request is evaluated against the requester's authenticated role, the data classification, and the operational context per CJIS Security Policy requirements. All access decisions are logged with the requested identity, timestamp, data category accessed, and disposition, creating a complete audit trail for privacy compliance review. Role-based access control is enforced with unique credentials and periodic access reviews aligned to CJIS standards.

4.4.10.2 Neb. Rev. Stat. and Federal Alignment

Privacy controls are designed to satisfy Nebraska state privacy requirements, including Neb. Rev. Stat. §86-125, and the FBI CJIS Security Policy. INDIGITAL's privacy framework is reviewed annually and updated whenever regulatory changes affect NG911 data handling obligations.

4.4.11 Security Assessment and Audit (§E.4.7)

INDIGITAL fully complies with RFP §E.4.7 Security Assessment and Audit. Our security posture is validated through a layered assessment program that combines continuous automated scanning, periodic penetration testing by independent third parties, and annual compliance audits against industry-recognized frameworks.

4.4.11.1 Penetration Testing

INDIGITAL engages an independent, qualified third-party firm to conduct penetration testing of the Nebraska ESInet and NGCS as detailed in the Vol 3 Work Plan (§3.3, Milestone M19). The scope covers external network penetration, internal network penetration, web application testing for all PSAP-facing portals and administrative interfaces, and security controls validation including firewall rule validation, IDS/IPS alert and block testing, mutual TLS boundary enforcement, RBAC access control verification, and encryption-in-transit validation. All findings are risk-rated using the CVSS v3.x framework, and remediation timelines are established based on severity: critical findings remediated as soon as possible, high within 30 days, medium within 60 days, and low within 90 days.

4.4.11.2 Vulnerability Scanning

Vulnerability scanning of all ESInet and NGCS production systems is conducted on a quarterly cadence at minimum, using industry-standard scanning tools including NESSUS, OpenVAS, and Rapid7 with CVSS v3.x scoring. Scan results feed directly into the SIEM for correlation with threat intelligence. Additional scanning is triggered by vendor CVE notifications, CISA DHS advisories, and open-source intelligence sources. Quarterly vulnerability assessment reports are provided to the Nebraska PSC summarizing scan findings, remediation status, and trend analysis.

4.4.11.3 External Compliance Audits

INDIGITAL engages independent auditors to validate security controls supporting the Nebraska NG911 system. Audit scope covers security, availability, processing integrity, confidentiality, and privacy. Audit reports are made available to the Nebraska PSC upon request.

4.4.11.4 Internal Audit Program

INDIGITAL conducts internal security audits at least annually, with external audits conducted at minimum once every three years. Internal audits verify that security controls are operating as designed, that access reviews have been completed, that patch compliance targets are met, and that incident response procedures remain current. An annual NG-SEC compliance matrix is completed to confirm ongoing alignment with NENA security requirements. Audit findings are reported directly to the CIO/CSO.

4.4.11.5 Risk Assessment

A formal risk assessment aligned with NIST SP 800-30 is conducted annually and whenever a significant change to the system occurs. Risk assessment results inform the security roadmap and are shared with the Nebraska PSC as part of the annual security review.

4.4.11.6 Assessment and Audit Documentation (§E.4.7.1)

INDIGITAL fully complies with RFP §E.4.7.1. All security assessment and audit activities produce structured documentation that will be retained, version-controlled, and available for Nebraska PSC review.

4.4.11.6.1 Documentation Inventory

The following documents are maintained as part of the assessment and audit program:

- Annual Penetration Test Report (scope, methodology, findings, remediation plan, and retest confirmation), aligned to the third-party testing approach described in Vol 3 §3.3.
- Quarterly Vulnerability Assessment Report (scan results from NESSUS, OpenVAS, and Rapid7, trending analysis, remediation status, exception justifications)
- External Compliance Audit Report (independent auditor findings, control descriptions, test results, and management responses)
- Annual Internal Audit Report (control effectiveness assessments, access review results, patch compliance metrics, NG-SEC compliance matrix, incident response drill outcomes)
- Annual Risk Assessment Report (threat landscape analysis, risk register updates, residual risk acceptance documentation)

- Remediation Tracking Log (all findings from any assessment source, with assigned owner, target remediation date, actual closure date, and evidence of corrective action).

4.4.11.6.2 Retention and Access

All assessment and audit documentation is retained for a minimum of six years for administrative and compliance records and three years for operational records, all in encrypted, access-controlled storage. The Nebraska PSC may request any document at any time during the contract period. INDIGITAL provides assessment status reporting to the Nebraska PSC showing open findings count by severity and remediation progress.

4.4.12 Intrusion Detection and Prevention (§E.4.8.3)

INDIGITAL fully complies with RFP §E.4.8.3 Intrusion Detection and Prevention Systems. IDS/IPS capabilities are deployed at every critical boundary and internal segment of the Nebraska ESInet and NGCS, providing both signature-based detection for known threats and behavioral analytics for zero-day and advanced persistent threats.

4.4.12.1 Deployment Architecture

Fortinet FortiGate firewalls with licensed IDS/IPS are deployed at all ESInet ingress and egress points (BCF locations), at the boundary between the ESInet transport layer and NGCS application layer, at all interconnects with Originating Service Providers, and at all management network access points. A third-party monitoring vendor provides an additional defense-in-depth layer at data centers, using layer 2 network monitoring for predictive analysis and full packet capture for forensic support after cyber incidents.

4.4.12.2 Detection Capabilities

The Fortinet FortiGate IDS/IPS platform combines multiple detection methodologies: signature-based detection using continuously updated rulesets from commercial and open-source threat intelligence feeds tuned for SIP, HTTP/HTTPS, and NG911-specific protocols; heuristic analysis and real-time threat intelligence feeds enabling detection of novel attack vectors including zero-day exploits, advanced targeted attacks, ransomware, polymorphic attacks, and SIP-specific threats (malformed INVITE floods, registration hijacking, RTP injection); and protocol analysis for deep inspection of SIP, HELD, LoST, and other NG911-specific protocols, detecting deviations from expected message structures.

4.4.12.3 Response and Integration

IDS/IPS alerts are forwarded in real time to the SIEM platform within INDIGITAL's Security Operations Center. Alert triage follows the severity classification and escalation procedures defined in the Incident Response Plan (§4.4.1). For high-confidence, high-severity detections, the IPS operates in inline blocking mode to automatically drop malicious traffic before it reaches protected NGCS components. All IPS blocking actions are logged with full packet capture for forensic review.

4.4.12.4 Tuning and Maintenance

IDS/IPS rulesets are reviewed and tuned regularly to reduce false positives while maintaining detection coverage. Tuning decisions are documented and reviewed during internal security audits. The INDIGITAL security team is responsible for ruleset management under the direction of the CIO/CSO.

4.4.13 DNS Security (§E.4.9)

INDIGITAL fully complies with RFP §E.4.9 Domain Name System Security. DNS is a critical infrastructure dependency for NG911 because the NENA i3 architecture relies on Fully Qualified Domain Names (FQDNs) for agency and agent identity, certificate validation, LoST/ECRF service discovery, and SIP routing. INDIGITAL's DNS architecture is designed for resilience, integrity, and protection against DNS-based attack vectors per NENA-STA-040 Section 6.4 and NIST CSF 2.0 PR.IP-01.

4.4.13.1 DNS Architecture and Resilience

DNS services supporting the Nebraska NG911 system are deployed across INDIGITAL's geographically diverse data center infrastructure with automatic failover, ensuring that DNS resolution remains available even during a facility-level outage. Recursive resolvers serving NGCS components are configured to resolve within the NG911 trust domain, limiting exposure to external DNS threats.

4.4.13.2 DNS Threat Mitigation

INDIGITAL's DDoS protection framework extends to DNS-specific attack vectors. The solution tracks unique identifiers specific to trusted DNS servers and refuses DNS responses carrying different identifiers, preventing spoofed DNS responses from reaching NG911 components. Secure DNS is implemented via encrypted ports where available, mitigating interception and manipulation of DNS queries in transit. DNS query anomalies are monitored and correlated through the SIEM alongside other security events, and ingress filtering at the BCF layer provides an additional defense against DNS amplification and reflection attacks.

4.4.13.3 Integration with NG911 Services

DNS underpins several NG911 functional elements: the ECRF and LVF rely on DNS-based service discovery for LoST protocol resolution, SIP routing uses DNS NAPTR and SRV records for next-hop determination, and the PKI framework uses DNS for certificate validation and chain-of-trust verification. All of these critical-path dependencies are served by INDIGITAL's secure DNS infrastructure with no reliance on public DNS resolvers.

4.5 Standards Conformance Narrative (§B.3)

RFP §E: Explain in detail how the proposed solution conforms to all standards listed in §B, including NENA-STA-010.3, NENA-STA-040.2-2024, FCC 47 CFR Part 9, and all other referenced documents. Mandatory per RFP – the State may disqualify non-conformant proposals.

INDIGITAL's proposed ESInet and NGCS solution conforms to all standards referenced in RFP §B and §E. This section provides an explicit conformance statement for each required standard, maps it to the relevant technical section of this volume, and identifies the compliance posture (Full Comply, Comply with Addendum clarification, or Phased delivery where the RFP itself provides a timeline).

Standard	Scope	Conformance	Vol. 4 Reference
NENA-STA-010.3-2021(i3 Standard)	Full ESInet and NGCS architecture, interfaces, call flows, functional elements, data models, APIs, and security trust model	Full Comply – production-deployed across multiple statewide deployments	§4.1, §4.2, §4.3, §4.4
NENA-STA-040.2-2024(NG9-1-1 Security)	Security architecture across all 9 NG-SEC domains; HSM, PKI, RBAC, cryptography, threat response	Full Comply – FIPS-aligned; HSM for CA/root keys; independent pen test	§4.4
NENA-STA-006.2-2022(GIS Data Model)	GIS data schema for PSAP boundaries, ESN boundaries, address points, civic addressing, routing attributes	Full Comply – DIG enforces schema compliance on all GIS data ingestion	§4.3
NENA-STA-034.1-2022(Legacy Gateways)	LNG, LSRG, LPG functional requirements and interfaces	Full Comply – all three gateway types implemented	§4.1.3
NENA-STA-015.10(Logging)	Logging service functional requirements, CDR fields, secure storage, RBAC access	Full Comply – logging addressed in §4.8 (Reporting Services) and Volume 2 Section 2.7	§4.8
NENA-STA-010.3	Additional Data Repository functional requirements	Full Comply – ADR described in §4.2.4	§4.2.4
RFC 3261 / RFC 9071(SIP)	Core SIP and NG911 SIP extensions for emergency call signaling	Full Comply	§4.1.1, §4.2.5
RFC 5222(LoST)	Location-to-Service Translation protocol for ECRF routing	Full Comply	§4.2.3 (ECRF)
RFC 4119 / RFC 5139(PIDF-LO)	Location Object format for location conveyance	Full Comply	§4.3.2
IEEE std. 1588-2008 (PTP) / RFC 5905(NTP)	Network time synchronization to within $\pm 1\text{ms}$ across all nodes using redundant	Full Comply	§4.1.4

Standard	Scope	Conformance	Vol. 4 Reference
	hardware clocks supporting PTP and NTP. All Data Center clocks are synchronized to Master in Ft Wayne Data Center and public NIST clocks as backup.		
RFC 4575(SIP Conference)	Conference event package for bridge and transfer	Full Comply	§4.2.5 (Bridge)
FIPS 140-3	Cryptographic module validation for HSM and endpoint TLS; required where RFP specifies; preferred otherwise (Q&A #34)	Comply – HSM FIPS-validated; endpoint modules FIPS-aligned	§4.4.4
FCC Report and Order 13-158	911 reliability requirements: router diversity, geographic diversity, single-point-of-failure elimination	Full Comply – dual-manufacturer routers per node; geographic diversity across all nodes	§4.1.5
FCC 47 CFR Part 9	FCC requirements for 911 service obligations and interconnection	Full Comply	§4.1, §4.2
NENA-INF-016.2-2018(ESIND)	ESInet design guidance document	Comply – design follows ESIND recommendations throughout	§4.1

For each standard above, the Technical Matrix (Appendix B) contains the row-level compliance designation (Comply, Custom, or 3rd Party) and a cross-reference to the specific section of this proposal where the requirement is addressed. The 'Section in Response' column of the Technical Matrix references Volume 4 sections by number for all technical requirement rows.

4.6 Router Diversity and Network Redundancy (§E.1.5)

RFP §E.1.5.2: 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.

INDIGITAL's ESInet fully complies with the router diversity requirement confirmed in RFP §E.1.5.2 and Addendum 2, Q&A #11. At every ESInet node in the Nebraska deployment, we deploy at least two physical network routers from different manufacturers. This requirement is not aspirational – it is a design constraint enforced in our standard ESInet architecture, reflecting our recognition that equipment diversity is a fundamental reliability principle for life-safety infrastructure.

4.6.1 Dual-Manufacturer Router Architecture

The confirmation provided in Addendum 2; Q&A #11 is explicit: each ESInet node must utilize at least two physical network routers from different manufacturers. This is equipment and vendor diversity – not circuit diversity (which is also implemented separately). The two-manufacturer design ensures that:

- A firmware defect specific to one router platform cannot simultaneously disable both routing paths at a node.
- A hardware recall or supply chain vulnerability affecting one manufacturer cannot reduce redundancy to zero at any node.
- A vendor-specific vulnerability – including zero-day exploits, backdoors, or supply chain compromises – affecting one platform, is automatically isolated by the presence of the diversely sourced second router.

INDIGITAL's proposed router platform pairings for Nebraska ESInet nodes are:

4.6.1.1 Cisco

- **Role:** Primary vendor for routing and switching infrastructure.
- **Expertise:** INDIGITAL has extensive experience with Cisco products, supported by a team of technicians proficient in their deployment and management.
- **Reliability:** Cisco routers ensure robust routing paths, contributing to overall system reliability and compliance with FCC standards.

4.6.1.2 Arista

- **Role:** Alternate vendor for routing and switching solutions.
- **Strengths:** Known for high-performance networking capabilities, Arista provides additional redundancy and flexibility in system architecture.
- **Integration:** Their hardware complements Cisco offerings, enhancing overall network resilience and performance.

4.6.1.3 Fortinet

- **Role:** Alternate vendor focused on security and network appliances.
- **Features:** Fortinet's products strengthen INDIGITAL's security posture, addressing vulnerabilities and providing essential protection for network infrastructure.
- **Collaboration:** Works alongside Cisco and Arista to create a comprehensive and secure networking environment.

4.6.2 Three-Dimensional Diversity

Router diversity is one component of INDIGITAL's three-dimensional reliability strategy:

- Geographic diversity: ESInet nodes are distributed across geographically separate locations with no single geographic failure zone able to disable more than one node.
- Technology diversity: Core routing functions use different protocol implementations and hardware architectures to eliminate common-mode failures in the technology stack.
- Vendor diversity: Physical routers from at least two different manufacturers at every node, per §E.1.5.2.

This three-dimensional approach ensures that no combination of geographically correlated event, technology-specific failure, and manufacturer-specific vulnerability can simultaneously disable redundant routing paths at any Nebraska ESInet node. A 'backhoe incident' that severs a physical circuit does not disrupt 911 service because diverse physical routing is in place. A router manufacturer's critical firmware defect does not reduce routing capacity to zero because the second router at every node is from a different manufacturer.

4.6.3 FCC Report and Order 13-158 Conformance

INDIGITAL's ESInet reliability design conforms to FCC Report and Order 13-158, which establishes national 911 network reliability standards aimed at enhancing 911 reliability across all communication networks. FCC R&O 13-158 conformance is not a checkbox — it is the operational baseline from which our reliability architecture was designed, and Nebraska's PSAPs are the direct beneficiaries of a network built to this standard.

4.7 In-State Data Center Response

RFP §E.2: 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.

4.7.1 Proposed Data Center Architecture

INDIGITAL's proposed architecture uses a minimum of three data centers: two in-state Nebraska facilities providing the primary and secondary active-active core, plus one geographically distant facility more than 100 miles away (outside Nebraska) providing a disaster recovery tier with geographic separation sufficient to prevent common-cause failures from severe weather, regional power events, or other localized incidents that could affect both Nebraska facilities simultaneously.

4.7.2 Why In-State Infrastructure Matters for Nebraska

The Addendum 2, Q&A #22 response identifies three State-articulated reasons for in-state preference: improved jurisdictional control and ease of coordination with stakeholders; potentially lower latency and better performance for in-state PSAPs; and enhanced resiliency and geographic diversity when combined with an additional diverse site. INDIGITAL's architecture directly addresses all three:

- Jurisdictional control: Nebraska's call records, location data, and configuration data reside in Nebraska. The PSC and 911 Advisory Committee can audit, inspect, and

coordinate with the data center operator within Nebraska's legal jurisdiction without navigating out-of-state privacy or discovery frameworks.

- Latency: Round-trip latency from Nebraska PSAPs to in-state data centers is materially lower than latency to out-of-state facilities, reducing SIP transaction round-trip times for ESRP routing, ECRF lookups, and LIS queries. Lower latency directly improves call setup time for Nebraska's 954,417 annual calls.
- Geographic diversity: Two in-state Nebraska facilities, separated by sufficient distance to avoid common-cause weather and infrastructure events, provide Nebraska-specific geographic redundancy. Combined with the geographically distant third facility, this architecture delivers both in-state resilience and out-of-state disaster recovery in a single architecture.

4.7.3 Evaluation Scoring Impact

Per Addendum 2, Q&A #7, in-state versus out-of-state data center placement is evaluated as part of the overall technical score, including resiliency, latency, and risk. It is one factor among several. INDIGITAL's commitment to both primary data centers being in Nebraska represents the strongest possible response to this preference — not merely meeting the minimum of one in-state facility but anchoring the entire primary infrastructure in Nebraska. This architectural choice reflects INDIGITAL's long-term commitment to Nebraska's 911 system, not a procurement optimization for a single evaluation criterion.

4.8 Reporting Services Requirements (§E.5)

RFP §E.5: "The Contractor shall provide comprehensive reporting and logging services across all ESInet and NGCS functional elements, including enterprise-wide logging conformant with NENA-STA-010.3, i3 Logging and Reporting Requirements, Functional Element Reporting for all required element types, Monitoring and Outage reporting, Maintenance and Configuration reporting, and Discrepancy Reporting for all defined report categories."

INDIGITAL fully complies with all requirements set forth in RFP §E.5 Reporting Services Requirements. Reporting and logging are not optional capabilities added to our platform. They are first-class functions built into the core architecture of the Nebraska ESInet and NGCS from the ground up, operated continuously through our 911 Logix Location Integrity Oversight Service (LIOS), and accessible to Commission staff through a role-appropriate reporting portal at all times.

The State has recently awarded a separate logging service contract. INDIGITAL acknowledges this arrangement and, consistent with Addendum 2, Q&A #42, will provide the data access interfaces and feeds necessary for the separately awarded contractor to retrieve NG911 system data. Any interface or data access fees associated with this integration are reflected in Appendix A pricing.

4.8.1 Reporting and Data Collection Requirements (§E.5.1)

RFP §E.5.1: "The Contractor shall provide an enterprise-wide logging and reporting system that is agnostic to provider, system, and technology. The system shall collect statewide and PSAP-level data and shall generate all LogEvent types defined in NENA-STA-010.3."

INDIGITAL's reporting architecture collects data across every functional element of the Nebraska ESInet and NGCS without dependency on the specific CHE platform, OSP technology,

or legacy gateway type at any PSAP. Every element that generates a LogEvent under NENA-STA-010.3 sends that event to the logging infrastructure in real time. No call, no routing decision, and no system state change is invisible to the reporting system.

Data collection operates at two levels. At the statewide level, aggregate metrics covering all 68 Nebraska PSAPs, all 7 regions, and all functional elements are available in a single dashboard view. At the PSAP level, Commission staff and authorized agency personnel can drill to individual PSAP call volumes, answer times, routing accuracy, and connectivity status. Role-based access controls govern which data views are available to each user class, consistent with the privacy and security requirements in RFP §E.4.

4.8.2 Logging Service (§E.5.2)

RFP §E.5.2: "The Logging Service shall conform to NENA-STA-010.3 requirements and shall log all LogEvents including media. The service shall be available to any PSAP implementing i3 logging interfaces and shall support ElementState and ServiceState SUBSCRIBE/NOTIFY per NENA-STA-010.3."

INDIGITAL's Logging Service, deployed through our 911 Logix LIOS partnership, is fully conformant with NENA-STA-010.3. The service logs all call LogEvents including voice, Real-Time Text (RTT), video, and supplemental data events. Every PSAP connected to Nebraska's ESInet can access the logging service through standard i3 logging interfaces without requiring PSAP-specific integration work.

ElementState and ServiceState SUBSCRIBE/NOTIFY is supported for all ESInet and NGCS functional elements. PSAPs and authorized monitoring systems can subscribe to receive real-time state change notifications for any element in the Nebraska system, including availability transitions, degraded-mode entries, and restoration events. The logging service retains all events for the full contract term with secure, encrypted, tamper-evident storage.

4.8.3 i3 Logging and Reporting Requirements (§E.5.3)

RFP §E.5.3: "The Contractor shall implement all functional element logging, data collection, and reporting per NENA-STA-010.3, including query, retrieval, and log event replicator mechanisms."

Every NGCS functional element deployed in Nebraska generates the complete set of LogEvents it is required to produce under NENA-STA-010.3. This includes the BCF, ESRP, ECRF, LVF, LIS interface, Forest Guide, ADR, and all gateway elements. Log completeness is monitored by the NSOC using automated coverage checks that flag any element whose LogEvent generation rate deviates from baseline.

The log event replicator mechanism allows the Commission's separately awarded logging service contractor to receive a real-time or scheduled replica of all LogEvents generated by the Nebraska ESInet and NGCS. The replication interface is implemented using the standard NENA-STA-010.3 log replication protocol, ensuring interoperability with any compliant logging analysis platform. Query and retrieval interfaces are available via REST API with role-authenticated access, enabling Commission staff to retrieve historical log data for any time window within the retention period.

4.8.4 Functional Element Reporting (§E.5.4)

RFP §E.5.4: "The Contractor shall provide all required functional element report types as defined in NENA-STA-010.3 §7.6, including ESRP, ECRF, LVF, LIS, BCF, LNG, SIP Conference, PSAP

Routing Duration, Concurrent Calls, BCF/ESRP Session Reporting, and ESRP Queue State reporting."

INDIGITAL generates all ten required functional element report types for the Nebraska NGCS. The following table describes each report type, the generating element, the reporting frequency, and the delivery mechanism.

ESRP Routing Report: Generated by the ESRP for every call processed. Contains the originating OSP, PIDF-LO location used for routing, PSAP destination URI, policy rule applied, and routing decision timestamp. Available in the reporting portal and exportable via API in JSON and CSV formats. Delivered continuously; summary reports generated on a configurable schedule.

ECRF Query Report: Generated by the ECRF for every LoST query received from the ESRP or any authorized querier. Contains the queried location, returned service boundary, PSAP URI, and query response time. Used to validate routing accuracy and identify location data quality issues. Available in real time through the NSOC monitoring dashboard.

LVF Validation Report: Generated by the LVF for every location validation request. Contains the location submitted, the validation result (valid, invalid, or borderline), and any discrepancy flag generated. Feeds directly into the GIS discrepancy reporting workflow described in Section 4.8.7.

LIS Interface Report: Documents all HELD protocol queries processed against the LIS interfaces of connected OSPs. It contains query timestamps, OSP identifier, response time, and any failed resolution events. Used to track OSP LIS performance and identify connectivity issues before they affect call routing.

BCF Session Report: Generated by the BCF for every SIP session admitted, rejected, or rate-limited at the ESInet boundary. Contains the originating IP address, session disposition, PASSporT attestation level, and any security event flags. Used by the SOC for threat analysis and by the NSOC for capacity monitoring.

LNG Gateway Report: Generated by the Legacy Network Gateway for all legacy OSP calls ingested, including CAMA and SS7 trunks, TTY-to-RTT conversions, and E2 interface events. Contains per-trunk call volumes, conversion success/failure rates, and gateway availability metrics.

SIP Conference Report: Generated by the Conference Bridge for all multi-party sessions, including PSAP-to-PSAP transfers, supervisor monitor sessions, and emergency responder conferences. Contains participant identities, session duration, EIDO transfer confirmation, and call metadata continuity status.

PSAP Routing Duration Report: Measures end-to-end call routing duration from the SIP INVITE entering the BCF to the call being delivered to the PSAP. Reported per PSAP, per region, and statewide. Used to verify that routing latency remains within SLA thresholds across all 68 Nebraska PSAPs.

Concurrent Calls Report: Real-time and historical reporting of concurrent active call sessions across the Nebraska ESInet. Reported by PSAP, region, and statewide, with peak concurrency tracking against provisioned capacity. Used for capacity planning and to verify that the 200 percent peak provisioning standard is being maintained as call volumes evolve.

ESRP Queue State Report: Reports the state of ESRP call queues including queue depth, longest-queued call duration, and dequeue rates by PSAP. Generated on a continuous basis and available in the real-time monitoring dashboard. ESRP Queue State data is used to trigger overflow routing when a PSAP queue exceeds its defined threshold.

4.8.5 Monitoring, Outages, Failover, Trouble Tickets, and Escalation (§E.5.5)

RFP §E.5.5: "The outage classification and escalation framework shall designate a single outage owner; any outage visible to a PSAP shall be reported to that PSAP and to the State. The Help Desk shall be staffed 24/7 with qualified technicians and shall answer 90 percent of calls within 60 seconds, with follow-up provided within 5 minutes for 99 percent of calls."

INDIGITAL fully complies with §E.5.5. Every outage affecting a Nebraska PSAP is assigned a single named owner in the NSOC ticket system at the moment of detection. Ownership does not rotate between technicians during an active outage. The assigned owner holds the ticket through resolution, ensuring continuous accountability and eliminating the ambiguity that occurs when outage response is shared across a team without a single point of responsibility.

60-Second Answer Commitment: 90 percent of all incoming calls to the INDIGITAL NSOC Help Desk are answered by a live, knowledgeable technician within 60 seconds. This is a firm operational commitment, not a target. All problem reports received by telephone, the call must be answered by a qualified technician within 60 seconds 90 percent of the time.

5-Minute Follow-Up Commitment: 99 percent of all calls requiring escalation or technical action receive a follow-up contact within 5 minutes of the initial answer. Follow-up contact means a direct communication to the reporting party, not a ticket status update. For website entered tickets, an initial automated email will be generated immediately, and a follow up email or telephone call must be sent within 5 minutes 99% of the time.

PSAP Outage Notification: Any outage or degradation event visible to a PSAP triggers an immediate proactive notification to that PSAP's designated contact within 15 minutes of NSOC detection. The Commission receives a simultaneous notification. PSAPs do not learn about outages affecting their 911 service from their own call takers.

Failover Reporting: Every automatic failover event in the Nebraska ESInet or NGCS generates a failover report to the Commission within 30 minutes of the event. The report identifies the triggering failure, the failover path activated, the recovery time, and the current system state. Failover events that trigger a redundancy loss (Category 2 alarm per Section 2.9.7) require a written root cause analysis within five business days.

4.8.6 Maintenance and Configuration Reports (§E.5.6)

RFP §E.5.6: "The Contractor shall provide maintenance event reports including details and corrective actions and change management reports integrated with operational reporting."

INDIGITAL generates a maintenance report for every planned and emergency maintenance event affecting the Nebraska ESInet or NGCS. INDIGITAL coordinates all planned maintenance activities with the Commission and affects PSAPs at least 10 business days (14 calendar days) in advance and post-event (confirming completion, any deviations from the MOP, and system state verification results). Emergency maintenance reports are issued within two hours of work completion.

Configuration change reports document every modification to the Nebraska system configuration, including hardware changes, software updates, routing policy changes, certificate renewals, and GIS data structural changes. Each configuration report identifies the change type, the specific element modified, the pre-change and post-change configuration baselines, the change authorization reference (CMB approval record), and the engineer who executed the change. Configuration reports are retained for the full contract term and are available to the Commission on request.

Audit trails generated by the configuration reporting system satisfy the three-year minimum retention requirement and provide forensic-quality records suitable for regulatory review. All configuration report data is available through the Commission reporting portal with the same role-based access controls that govern call record and log data access.

4.8.7 Discrepancy Reporting (§E.5.7)

RFP §E.5.7: "The Contractor shall provide discrepancy reporting tools and automated report generation for all defined report categories, including Policy and Core Routing discrepancies, Location and GIS Source discrepancies, Signaling and Edge discrepancies, and Test and Tools discrepancy reports."

INDIGITAL's discrepancy reporting framework covers all twelve report categories defined in RFP §E.5.7 and NENA-STA-010.3 §7.6. Discrepancy reports are generated automatically by the system when a condition requiring attention is detected and are also available for manual submission by PSAP personnel and Commission staff through the reporting portal. Every discrepancy report is routed to the appropriate resolution owner and tracked through closure.

Policy and Core Routing Discrepancies (§E.5.7.1)

Policy Store Discrepancy Report (§E.5.7.1.1): Generated automatically when the ESRP detects a policy inconsistency, a policy retrieval failure, or a conflict between routing policy and the active GIS boundary data. Routes to the INDIGITAL NGCS operations team for immediate resolution. Every Policy Store discrepancy is treated as a High or Critical event depending on whether active call routing is affected.

Policy Discrepancy Report (§E.5.7.1.2): Generated when a specific policy rule produces an unexpected routing outcome or fails validation. Contains the policy rule identifier, the input that triggered the discrepancy, the expected and actual routing outcomes, and the policy store version at the time of the event.

ESRP Discrepancy Report (§E.5.7.1.3): Generated by the ESRP when it encounters a call that cannot be routed to the correct PSAP due to a missing location, an unresolvable ECRF query, or a policy failure. Contains the full SIP INVITE headers, the PIDF-LO location data (or absence thereof), the ECRF query result, and the default routing action taken.

Location and GIS Source Discrepancies (§E.5.7.2)

LIS Discrepancy Report (§E.5.7.2.1): Generated when a HELD protocol query to an OSP LIS returns an error, a malformed PIDF-LO response, or a location that fails LVF validation. Routes to the relevant OSP for remediation with a copy to the Commission. LIS discrepancy rates are tracked by OSP and included in the Monthly Performance Report.

GIS Discrepancy Report (§E.5.7.2.2): Generated by INDIGITAL's DIG pipeline when a GIS data submission fails schema validation, contains a topology error (gap or overlap in PSAP boundary

data), or conflicts with an existing authoritative layer. Routes to the relevant county GIS authority and to GeoComm's spatial interface team for correction. GIS discrepancy reports are tracked through resolution by the LIOS platform with timestamped status updates.

MSAG Conversion Service Discrepancy Report (§E.5.7.2.3): Generated when the MSAG Conversion Service encounters an address that cannot be converted to NENA GIS format, a conflict between MSAG records and GIS address points, or a failed civic-to-geodetic geocoding result. Used to identify legacy address data quality issues requiring remediation before those addresses can be routed correctly in the NG911 environment.

LoST Discrepancy Report (§E.5.7.2.4): Generated by the ECRF when a LoST query returns a result indicating that the queried location falls in a gap area, an overlap area, or an area not covered by any PSAP service boundary in the current routing database. Routes to the GIS operations team and to the relevant county authority. LoST discrepancy reports are the primary mechanism for surfacing GIS coverage gaps before they cause misroutes on live 911 calls.

Signaling and Edge Discrepancies (§E.5.7.3)

SIP Discrepancy Report (§E.5.7.3.1): Generated by the BCF or ESRP when a SIP message fails validation, contains a malformed header that cannot be normalized, or exhibits behavior inconsistent with the NENA-STA-010.3 SIP profile for NG911. Routes to the affected OSP or PSAP with specific header-level detail to support rapid remediation.

BCF Discrepancy Report (§E.5.7.3.2): Generated when the BCF blocks a call or session due to a policy violation, a certificate validation failure, a rate limit breach, or an anomalous traffic pattern. BCF discrepancy reports feed directly into the SOC security event workflow. Patterns of BCF discrepancies are analyzed by the SOC for TDoS and SIP flooding indicators.

OSP and Test Tool Discrepancies (§E.5.7.4)

OSP Discrepancy Report (§E.5.7.4.1): Generated when an OSP interface produces a call with missing or invalid location data, a PASSporT validation failure, or a signaling deviation from the agreed interconnect specification. Routes to the affected OSP with specific call details for remediation. OSP discrepancy rates are tracked per OSP and reported to the Commission monthly.

Test Call Generator Discrepancy Report (§E.5.7.4.2): Generated when test call generators used for ongoing system validation produce unexpected results, including routing failures, location errors, or SIP signaling anomalies that were not present in the prior test cycle. Test call generator discrepancy reports are used to detect system regression between maintenance events and are reviewed by the NSOC engineering team at each weekly operational briefing.

4.9 Use Case Narratives (§E.10)

RFP §E.10: "Respondents shall provide use case examples demonstrating how their proposed solution handles normal call flow, abnormal call flow conditions, and failure scenarios. Use cases shall trace the end-to-end call path through all NGCS functional elements from origination through PSAP delivery, demonstrating standards conformance at each step."

INDIGITAL fully complies with RFP §E.10. The following use cases trace end-to-end call flows through Nebraska's ESInet and NGCS using specific Nebraska operational data, reflecting the actual system configuration proposed for this engagement. Each use case names the

functional element responsible at each processing step and identifies the NENA-STA-010.3 interface invoked. Three scenarios are presented: a normal wireless 911 call, an abnormal call with location resolution failure, and a PSAP failover scenario.

4.9.1 Normal Call Flow: Wireless 911 Call, Metro Region (§E.10.1)

RFP §E.10.1: "Describe the normal call flow for a wireless origination through the proposed ESInet and NGCS to PSAP delivery, including all functional element interactions, location delivery, and SIP header handling."

The following use case traces a wireless 911 call originating within Douglas County, Nebraska, the state's highest-volume PSAP region carrying approximately 53 percent of all statewide 911 call volume. The scenario demonstrates the complete normal call path through INDIGITAL's ESInet and NGCS from the moment the wireless handset initiates the call to the moment the call-taker at the Douglas County PSAP answers.

4.9.1.1 Step 1: Call Origination and OSP Handoff.

A caller dials 911 from a wireless handset on an i3-compliant carrier network operating in Douglas County. The carrier network establishes the caller's location using Phase II GPS coordinates and assembles a PIDF-LO Location Object with geodetic coordinates. The carrier initiates a SIP INVITE directed to the INDIGITAL ESInet's published IP Point of Interconnection (POI) for the Nebraska ESInet, using the configured SIP trunk established during system deployment.

4.9.1.2 Step 2: BCF Admission and Security Enforcement.

The SIP INVITE arrives at the INDIGITAL Border Control Function (BCF). The BCF performs mutual TLS authentication against the carrier's X.509 certificate, validates the STIR/SHAKEN PASSporT token in the Identity header, confirms the Resource-Priority header is set to the correct emergency class, applies rate limiting and anti-spoofing checks, and admits the session. The BCF inserts the NENA-Source parameter identifying the ESInet entry point and forwards the INVITE to the ESRP. Elapsed time from INVITE arrival to ESRP delivery: less than 50 milliseconds.

4.9.1.3 Step 3: ESRP Policy Evaluation.

The Emergency Services Routing Proxy (ESRP) receives the INVITE and extracts the PIDF-LO location from the SIP message body. The location is provided by value (geodetic coordinates embedded directly in the PIDF-LO). The ESRP checks the Policy Store for any active routing policy affecting calls from this carrier in this area (nonactive in this scenario) and initiates a LoST query to the ECRF with the geodetic coordinates.

4.9.1.4 Step 4: ECRF Location-Based Routing.

The Emergency Call Routing Function (ECRF) receives the LoST query containing the caller's geodetic coordinates. The ECRF performs a spatial query against the NENA GIS routing layers maintained by INDIGITAL's DIG pipeline, determines that the location falls within the Douglas County PSAP service boundary, and returns the Douglas County PSAP SIP URI (for example, sip:douglas@psap.ne.us) along with the service boundary polygon and a validity period. ECRF response time: less than 100 milliseconds.

4.9.1.5 Step 5: ESRP Call Routing to PSAP.

The ESRP receives the ECRF response, logs the routing decision (PSAP URI, location used, policy applied, timestamp) to the 911 Logix LIOS logging service, and routes the SIP INVITE to the Douglas County PSAP. All original SIP headers are preserved intact, including the P-Asserted-Identity, Resource-Priority, History-Info, and the PIDF-LO location body. The ESRP inserts the Call-Info header with the EIDO reference for supplemental data and confirms that the ESRP Queue State for Douglas County is open before delivery.

4.9.1.6 Step 6: PSAP Call Delivery and Answer.

The SIP INVITE is delivered to the Douglas County PSAP's Call Handling Equipment (CHE) at the configured SIP interface. The CHE presents the caller's location on the dispatcher's map, displays the PIDF-LO civic and geodetic location data, and triggers the ring at the next available call-taker position. The call-taker answers. Total time from carrier SIP INVITE to PSAP ring: less than 400 milliseconds under nominal conditions.

NENA-STA-010.3 interfaces exercised in this use case: BCF admission (§4.2.3), STIR/SHAKEN PASSporT validation (§7.4.10), ESRP policy routing (§4.2.2), ECRF LoST query and response (§4.3.1), PIDF-LO location conveyance (RFC 4119), ESRP call delivery with SIP header preservation (§4.2.4), and EIDO delivery (§5.2).

4.9.2 Abnormal Call Flow: Location Resolution Failure with Default Routing (§E.10.2)

RFP §E.10.2: "Describe the call flow for an abnormal condition such as a location resolution failure, demonstrating how the system handles the failure and routes the call to the appropriate default destination."

This use case traces a VoIP 911 call originating from a residential broadband customer in a rural Nebraska county where the OSP has not yet fully provisioned i3-compliant location services. The caller's registered address is in Dundy County, one of Nebraska's lowest-volume PSAPs at 581 annual calls and one position. The scenario demonstrates how INDIGITAL's system handles a location failure without dropping the call or routing it to a remote default PSAP.

4.9.2.1 Step 1: SIP INVITE with Incomplete Location.

The caller dials 911. The VoIP carrier sends a SIP INVITE to the INDIGITAL ESInet BCF, but the PIDF-LO in the SIP body contains only a civic address without geodetic coordinates. The civic address references the subscriber's registered service address in Dundy County, but the MSAG-format address has not yet been converted to a NENA GIS-conformant address point in the LDB.

4.9.2.2 Step 2: BCF Admission and LVF Validation Attempt.

The BCF admits the call (certificate and signaling are valid) and passes the INVITE to the ESRP. The ESRP extracts the PIDF-LO, passes the civic address to the LVF for validation. The LVF queries the LDB and finds that the address cannot be matched to a NENA GIS address point. The LVF returns a validation failure with a LoST discrepancy event logged to the LIOS reporting platform. A GIS Discrepancy Report is automatically generated and routed to the GIS operations team for address remediation.

4.9.2.3 Step 3: ECRF Default Routing.

The ESRP, having received a location validation failure, invokes the fallback routing path specified in the Policy Store for Dundy County civic addresses. The ECRF is queried with the county identifier extracted from the incomplete civic address. The ECRF returns the Dundy County PSAP URI as the default routing destination, consistent with the county-level default routing rules configured during system deployment. The call is delivered to the Dundy County PSAP with a location uncertainty flag in the SIP Call-Info header.

4.9.2.4 Step 4: PSAP Delivery with Location Warning.

The call is delivered to the Dundy County PSAP. The CHE presents the subscriber's registered address from the LDB as the best-available location indicator, with a visible warning that the location could not be geodetically validated. The dispatcher answers and immediately requests a callback location confirmation from the caller. The ESRP Discrepancy Report generated in Step 2 is reviewed by the INDIGITAL GIS team, and the Dundy County address point is added to the NENA GIS address layer within the standard remediation SLA.

This use case demonstrates that INDIGITAL's system never drops a 911 call due to a location failure. The call is always routed to the best-available PSAP using available location indicators, the PSAP receives a clear indication of the location uncertainty, and the underlying data quality issue is automatically flagged for remediation in the same processing pipeline that handled the call.

4.9.3 Failure Scenario: ESInet Node Failure with Automatic Failover (§E.10.1)

RFP §E.10.1: "Describe the system's behavior during a failure condition, including how the system detects the failure, activates redundancy, and maintains or restores 911 service without PSAP intervention."

This use case traces the system response when the primary Nebraska in-state data center loses power during peak operating hours, affecting the primary ESInet core node. The scenario demonstrates that no Nebraska PSAP loses 911 service and no call in progress is dropped.

4.9.3.1 T+0: Power Loss at Primary Data Center.

A power distribution failure at the primary Nebraska data center causes an immediate loss of power to the primary ESInet core node, including the primary BCF instances, ESRP instances, and ECRF read replicas at that facility. UPS power sustains network connectivity for the configured hold time (seconds) while the facility power management system attempts restoration.

4.9.3.2 T+3 seconds: Health Check Failure Detection.

The secondary data center's health monitoring agents detect that the primary BCF and ESRP instances have stopped responding to health check probes. The threshold for failover activation is two consecutive missed health checks at the configured interval. The monitoring system confirms the failure is not a transient probe issue by verifying that traffic flow from the primary site has also stopped. Failover activation is triggered automatically without operator intervention.

4.9.3.3 T+4 seconds: Active-Active Failover Activation.

The secondary data center's BCF and ESRP instances, which have been continuously processing their share of Nebraska call traffic in active-active configuration, absorb the full root cause Nebraska call load. Because the architecture is active-active, the secondary instances are already operational and processing calls. There is no cold-start delay. Calls in progress that were being handled by the primary instances are maintained through the ESRP call state replication mechanism. The RPO for call state is less than one minute, meaning any call that was in the signaling phase at the moment of failure is re-established within the recovery window.

4.9.3.4 T+5 seconds: RTO Achievement.

All new 911 calls arriving at the Nebraska ESInet are being processed exclusively by the secondary data center. All 68 Nebraska PSAPs continue to receive and answer 911 calls without interruption. The five-second RTO target is met. No PSAP experiences a call delivery failure. No dispatcher intervention is required at any PSAP.

4.9.3.5 T+15 minutes: NSOC Notification and Incident Response.

The NSOC generates a Category 1 (Critical Outage) alarm for the primary data center facility failure. The Commission's designated contact receives a notification within 15 minutes of identification of the failure event. An incident ticket is opened with the facility operator and with INDIGITAL's field engineering team. The NSOC monitoring dashboard shows all 68 Nebraska PSAPs in a "Degraded Redundancy" state (Category 2) rather than "Outage" because service is maintained, but the primary redundancy layer is unavailable.

4.9.3.6 T+ongoing: Redundancy Restoration.

INDIGITAL engineering works with the data center facility operator to restore primary site power and bring the primary ESInet core node back into service. Once the primary node is restored and validated, call traffic is rebalanced across both data centers. A failover event report is provided to the Commission within 30 minutes of the original event, and a root cause analysis is delivered within five business days of incident closure.

This use case demonstrates the operational reality of INDIGITAL's active-active architecture. The theoretical RTO of less than five seconds reflects an actual design constraint built into the system from the ground up. Nebraska's Commission does not have to accept a vendor's promise about failover times. It can verify this scenario during the acceptance testing phase described in Volume 3, Section 3.3.

Appendix 4-A: ESInet and NGCS Port Mapping

RFP §E.1.7: "Complete port mapping documentation shall be provided covering all required TCP/UDP ports for all traffic-handling devices including ESInet interfaces, OSP connections, PSAP connections, and management plane interfaces. The port mapping shall reflect a secure traffic management posture with a default-deny policy."

INDIGITAL fully complies with RFP §E.1.7. The port mapping below documents all TCP and UDP ports used across the Nebraska ESInet and NGCS. The default posture for all interfaces is deny-all except as explicitly listed. All unlisted ports are blocked at the BCF and perimeter firewall layers. If additional equipment interfaces and port connections are required, this list will be

reviewed and updated prior to implementation. This table will be maintained in the INDIGITAL Configuration Management Database (CMDB) throughout the contract term and updated within five business days of any architectural change affecting port assignments.

Interface / Element	Port(s)	Protocol	Direction	Purpose	Policy
BCF: OSP SIP Trunk Ingress	5061	TCP (TLS)	Inbound	SIP signaling from i3 OSPs over TLS (RFC 3261, NENA i3)	Allow from authorized OSP IP ranges only
BCF: OSP SIP Trunk Ingress	5060	UDP	Inbound	SIP signaling fallback for OSPs not yet on TLS (transitional)	Allow from authorized OSP IP ranges; disable post-transition
BCF: OSP Media (RTP/SRTP)	16384 - 32767	UDP	Inbound/Outbound	RTP and SRTP voice/video media streams from/to OSPs	Allow from authorized OSP IP ranges; SRTP enforced
BCF: STIR/SHAKEN STI-VS	443	TCP (TLS)	Outbound	HTTPS queries to STIR/SHAKEN verification service for PASSporT validation	Allow outbound to STI-VS endpoints
ESRP: PSAP SIP Delivery	5061	TCP (TLS)	Outbound	SIP INVITE delivery to PSAP CHE (mTLS required)	Allow to authorized PSAP IP addresses only
ESRP: PSAP Media (SRTP)	16384 - 32767	UDP	Inbound/Outbound	SRTP media streams to/from PSAP positions	Allow to/from PSAP IP ranges; SRTP required
PSAP: ElementState/ServiceState	5061	TCP (TLS)	Inbound	PSAP SUBSCRIBE/NOTIFY for ESInet service state per NENA-STA-010.3	Allow from authorized PSAP IP addresses
ECRF: LoST Query Interface	443	TCP (TLS)	Inbound	HTTPS LoST queries from ESRP, adjacent ESInets, and OSPs (RFC 5222)	Allow from ESInet-internal and authorized external LoST clients

Interface / Element	Port(s)	Protocol	Direction	Purpose	Policy
ECRF: Forest Guide	443	TCP (TLS)	Inbound/Outbound	Forest Guide recursive LoST queries for out-of-area resolution	Allow to/from authorized Forest Guide peers
LVF: Location Validation	443	TCP (TLS)	Inbound	HTTPS LVF validation queries from ESRP and authorized clients	Allow from ESInet-internal only
LIS: HELD Query Interface	443	TCP (TLS)	Outbound	HTTPS HELD queries to OSP LIS endpoints for location-by-reference (RFC 5985)	Allow outbound to authorized OSP LIS endpoints
ES-NNI: Adjacent ESInet SIP	5061	TCP (TLS)	Inbound/Outbound	SIP calls transferred to/from adjacent state ESInets via ES-NNI (mTLS)	Allow to/from authorized adjacent ESInet BCF IP addresses
LNG: CAMA/SS7 Trunk	5061	TCP (TLS)	Inbound	SIP signaling from Legacy Network Gateway for PSTN originations	Allow from LNG IP address; internal ESInet only
LSRG: Selective Router Interface	5060/5061	TCP/UDP	Inbound	SIP from Legacy Selective Router Gateway during transition period	Allow from LSRG IP range; expires post-transition
NSOC: SNMP Monitoring	161	UDP	Inbound	SNMPv3 polling from NSOC NMS to all managed ESInet elements	Allow from NSOC management IP range only; SNMPv3 required
NSOC: Syslog Collection	514	UDP	Outbound	Syslog event forwarding from all ESInet	Allow NSOC SIEM collector IP;

Interface / Element	Port(s)	Protocol	Direction	Purpose	Policy
				elements to NSOC SIEM	encrypted transport preferred
NSOC: NTP Synchronization	123	UDP	Outbound	NTP time sync to authoritative stratum-2 servers (RFC 5905)	Allow to authorized NTP server IPs only
Admin: SSH Management	22	TCP	Inbound	SSH access from NSOC and authorized INDIGITAL engineers (key-based auth only)	Allow from NSOC management subnet only; key auth required; no password auth
Admin: HTTPS Management UI	443	TCP (TLS)	Inbound	HTTPS access to element management interfaces; Commission reporting portal	Allow from NSOC and Commission portal IP ranges; MFA required
Admin: VPN Remote Access	4500/500	UDP (IPsec)	Inbound	IPsec VPN for authorized remote engineering access (MFA required)	Allow from authorized INDIGITAL engineer IP ranges only
PKI: OCSP Certificate Status	80/443	TCP	Outbound	OCSP queries for real-time certificate revocation status checks	Allow outbound to CA OCSP responder endpoints
PKI: CRL Distribution	80	TCP	Outbound	Certificate Revocation List download from CA distribution points	Allow outbound to CA CRL endpoints

All ports not listed above are blocked by default on all ESInet and NGCS boundary devices. The default-deny posture is enforced at both the BCF and the perimeter firewall layers, ensuring that

any new service or interface must be explicitly authorized through the Change Management Board process before traffic is permitted. Port policy changes are logged in the CMDB and included in the monthly configuration change report.

Appendix 4-B: FIPS 140-3 Cryptographic Module Inventory

RFP §E.4.4.1: "Cryptographic keys shall be protected using FIPS 140-2 validated cryptographic modules. The Contractor shall maintain an inventory of all cryptographic modules used in the solution, including the FIPS validation certificate number and the function served by each module."

Addendum 2, Q&A #34: "Where the RFP calls for FIPS-validated cryptography, cryptographic modules used to satisfy those requirements must have the appropriate FIPS validation. For modules or use cases where the RFP does not explicitly require FIPS validation, such validation is preferred but not mandatory."

INDIGITAL fully complies with RFP §E.4.4.1 and Addendum 2, Q&A #34. INDIGITAL will maintain an inventory identifying every cryptographic module used in the Nebraska ESInet and NGCS deployment, its FIPS 140-3 validation status, the specific function it serves, and the validation certificate number where applicable. FIPS 140-3 is fully backwards compatible with FIPS 140-2. The certificate numbers will be verified against the current NIST Cryptographic Module Validation Program (CMVP) database. This inventory will be maintained by Robert Brown, CIO/CSO, and updated whenever a module is added, replaced, or re-certified.

Appendix 4-C: Cross-Reference to Volumes 2 and 3

Several RFP sections within Appendix E address topics that span multiple proposal volumes. The following cross-references direct evaluators to the primary treatment of these topics in INDIGITAL's response.

§E.6 — Installation (Volume 3, Section 3.2)

The installation approach for the Nebraska ESInet and NGCS is addressed in Volume 3, Work Plan, Section 3.2, which details the phased installation schedule, site preparation requirements, equipment deployment procedures, and acceptance testing milestones for all 68 Nebraska PSAPs. Installation-related security controls, including physical access during deployment and secure configuration baselines, are addressed in this volume at §4.4.3 (Physical Security) and §4.4.4 (Cryptography and Secure Configuration).

§E.7 — Training (Volume 3, Section 3.4)

INDIGITAL's training program is addressed in Volume 3, Work Plan, Section 3.4, which describes the training curriculum, delivery methods, scheduling, and role-based training tracks for PSAP personnel, system administrators, and Commission staff. Security awareness training specific to the NG911 environment is referenced in this volume at §4.4.2.7 (Training and Exercise Evidence).

§E.8 — Operations and Service Management (Volume 2, Section 2.3)

Ongoing operations and service management are addressed in Volume 2, Qualifications and Experience, Section 2.3, which describes INDIGITAL's National Service Operations Center (NSOC) staffing model, service level commitments, incident management procedures, and

continuous improvement processes. The security monitoring and incident response components of operations are addressed in this volume at §4.4.8 (Security Monitoring, Detection, and Alerting) and §4.4.2 (Incident Response Plans).

§E.9 — Project Management (Volume 3, Section 3.1)

Project management methodology, governance structure, and milestone tracking are addressed in Volume 3, Work Plan, Section 3.1. This includes the project organizational chart, communication plan, risk management approach, and change management procedures. Security-related project milestones, including Milestone M19 (Security Testing and Penetration Test), are detailed in Volume 3, Section 3.3.

VOLUME 5: Terms and Conditions

5.1 TERMS ACCEPTANCE / EXCEPTION TABLE

Bidder should read the Terms provided with this RFP and must initial either "Accept All Terms and Conditions Within Section as Written" or "Exceptions Taken to Terms and Conditions Within Section as Written" in the table below (or include the same table in their solicitation response). If the bidder takes any exceptions, they must provide the following within the "Exceptions" field of the table; if an exception is not explicitly taken, it is deemed to be accepted as stated. Exceptions must include: 1. The specific clause, including section reference, to which an exception has been taken; 2. An explanation of why the bidder took exception to the clause; and 3. Provide alternative language to the specific clause within the solicitation response. — RFP Proposal Instructions §7, p. 112

INDIGITAL fully accepts all terms within Solicitation No. 202691101 as written. No exceptions are taken. INDIGITAL has initialed the "Accept All Terms Within Section as Written" column of the table provided on page 112 of the RFP, reproduced below, and authorizes the signatory on the Contractual Agreement Form to confirm this acceptance on behalf of the organization.

Accept All Terms within Section as Written (initial)	Exceptions Taken to Terms Within Section as Written (Initial)	Exceptions: (Bidder must note the specific clause, including section reference, to which an exception has been taken, an explanation of why the bidder took exception to the clause, and provide alternative language to the specific clause within the solicitation response.)
JH Authorized Signatory	N/A	INDIGITAL takes no exception. All terms within this solicitation are accepted as written.

Clarification Note (Addendum 2, Q&A #15 and #16). Addendum 2 Q&A #15 confirmed that the use of the word "terms" throughout this solicitation refers to the technical terms and defined requirements, not a separate standalone Terms and Conditions document. Formal Terms and Conditions will be provided by the Commission post-award to the selected vendor and will be negotiated at that stage. INDIGITAL accepts all technical requirements, defined terms, and requirements language as written throughout the solicitation, including all RFP sections, the Glossary, and all provisions incorporated by Addendum 1 and Addendum 2.

5.1.1 Deliverable Approval Process

Addressed here per Addendum 2, Q&A #3. Per Q&A #3, the Deliverable Approval Process is governed by the Terms section and must be addressed in the Response to Terms. RFP Section D confirms that all system and documentation deliverables are subject to this process.

INDIGITAL proposes the following framework, which will be incorporated into the final contract terms negotiated post-award.

INDIGITAL delivers on its commitments with the same accountability it brings to the 911 networks we operate. Our Deliverable Approval Process is structured to give the Nebraska Public Service Commission clear visibility, adequate time for thorough review, and a straightforward path to acceptance at each milestone. The process is designed to eliminate surprises, maintain schedule momentum, and ensure that every deliverable meets the Commission's stated acceptance criteria before being closed.

5.1.1.1 Submission and Notification

Upon completing each deliverable identified in RFP Section D, INDIGITAL will deliver the deliverable in electronic format to the Commission's designated Project Manager (PM) and will simultaneously submit a written Deliverable Submission Notice. The Notice will include the deliverable title and Section D reference number, the submission date and time, a brief description of the deliverable contents, a confirmation that all specified requirements have been addressed, and the name and contact information of the INDIGITAL PM of record for that submission.

5.1.1.2 Commission Review Period

Following delivery, the Commission will have ten (10) business days to review the deliverable and provide a written response. INDIGITAL acknowledges that the Commission may adjust this period in the final contract for deliverables of exceptional scope or complexity, and we will accommodate reasonable modifications to the review timeline with the Commission's written agreement.

5.1.1.3 Acceptance and Rejection

Upon completing its review, the Commission will issue one of the following responses in writing:

- **Written Acceptance:** The deliverable is accepted as submitted. INDIGITAL will log the acceptance date and close the deliverable in the project management system.
- **Written Notice of Deficiencies:** The Commission identifies specific deficiencies by requirement reference and provides a detailed written description of each. INDIGITAL will remedy all identified deficiencies and resubmit within five (5) business days of receiving the notice, unless a longer period is mutually agreed in writing.
- **Deemed Acceptance:** If the Commission does not respond within the review period and has not requested an extension in writing, the deliverable will be deemed accepted as of the close of business on the final day of the review period.

5.1.1.4 Escalation and Dispute Resolution

If INDIGITAL and the Commission disagree on whether a deficiency has been adequately remediated, the matter will be escalated to the INDIGITAL COO and the Commission's designated executive sponsor within two (2) business days of the resubmission. Both parties will make good-faith efforts to resolve the dispute within five (5) business days of escalation. INDIGITAL's COO will be personally available for escalation calls within 24 hours of notification, consistent with the lean, accountable support model we offer to every state we serve.

5.1.1.5 Single Point of Contact

INDIGITAL's Nebraska PM will serve as the single point of contact for all deliverable submissions, notices, and approvals. The PM's name, phone number, and email address will be confirmed at contract kick-off and communicated to all Commission stakeholders. Any changes to the PM assignment require the written approval of the Commission, consistent with RFP Proposal Instructions §1.i.

5.2 LICENSE, USER AGREEMENTS, AND SLAS

The bidders should submit with their solicitation response any license, user agreement, service level agreement, or similar documents that the bidder wants incorporated in the Contract. The Commission will not consider incorporation of any document not submitted with the solicitation response as the document will not have been included in the evaluation process. These documents shall be subject to negotiation and will be incorporated if agreed to by the Parties. – RFP Proposal Instructions §7, p. 112

INDIGITAL is not submitting any supplemental license agreement, user agreement, service level agreement, or similar document for incorporation into the final contract at this time. INDIGITAL acknowledges that the Commission will not consider incorporation of any document not submitted with this solicitation response.

INDIGITAL's approach to service levels, operational commitments, and system acceptance criteria is described in detail in Volume 2, Section 2.8 (Operational Support and SLA Response) and Volume 3, Section 3.3 (Testing and Acceptance Plan). These narratives reflect INDIGITAL's proposed operational framework and will serve as the basis for SLA negotiation during post-award contract finalization, consistent with Addendum 2 Q&A #6 and #16.

INDIGITAL looks forward to working collaboratively with the Nebraska Public Service Commission to develop final Terms and Conditions that are specific to the system procured, equitable to both parties, and protective of Nebraska's 911 infrastructure and the communities it serves.

Appendix A: Resumes

Shawn Walker, PMP

Project Manager | Proposal Role: **Project Manager**

Shawn Walker is a public safety and project management professional with more than 30 years of experience spanning PSAP operations, NG911 implementations, and enterprise-level technology deployments. She has directed complex, multi-agency projects across both the public and private sectors, with a career defined by cross-functional team leadership, operational improvement, and disciplined project execution. Shawn holds a Project Management Professional (PMP) certification and brings hands-on experience with NG9-1-1 Core Services (NGCS), ESInet implementations, CAD/RMS systems, and PSAP consolidation efforts. Her background as both a field-level practitioner and senior program manager makes her an effective liaison between technical teams and the public safety stakeholders they serve.

Academic Background

Master of Public Administration, Information Systems — State University of New York

Bachelor of Science, Organizational Management — Roberts Wesleyan College, Rochester, NY

Professional Certifications

Project Management Professional (PMP) Project Management Institute

Professional Experience

Role	Organization	Description
Project Manager / Technical Consultant 2025–Present	TSSI Consulting / INDIGITAL Telecom	Serves as Project Manager and Technical Consultant supporting the deployment of NG911 Next Generation Core Services for Missouri counties, enabling IP-based 9-1-1 call delivery via ESInet connections. Manages all phases of project execution including planning, requirements development, vendor coordination, and implementation oversight. Provides subject matter expertise in public safety operations, project management, and technology implementation.
Project Manager III 2020–2025	CentralSquare Technologies, Lake Mary, FL	Managed a portfolio of enterprise-level public safety software implementations for state and local agencies, including on-premise and cloud-based CAD and Records Management System (RMS) deployments. Led all phases of project management using Waterfall, Agile, and hybrid methodologies.

Role	Organization	Description
		Served as executive escalation point for client issues and reported portfolio performance to senior leadership.
Senior Project Manager 2016–2019	MAXIMUS, Rochester, NY	Led end-to-end enterprise implementations of healthcare services software for government clients. Supervised and mentored a team of project managers and developed new operational processes and performance improvement frameworks.
Group Leader / Senior Project Manager 2004–2016	L.R. Kimball, Ebensburg, PA	Led a team of project managers supporting state and local public safety agencies across a diverse portfolio including 9-1-1, NG9-1-1, PSAP consolidation, CAD/RMS, and land mobile radio (LMR) system selections and implementations. Authored more than 50 complex assessment reports and presented findings to state legislatures and local government leaders on PSAP regionalization strategies.

References: Available upon request.

Kent Claussen

Chief Technical Officer | Proposal Role: **Technical Lead**

Kent Claussen is a telecommunications engineering leader with deep technical expertise in network architecture, systems design, and public safety infrastructure. As Chief Technical Officer at INDIGITAL, he bears technical authority over the company's ESInet and Next Generation Core Services (NGCS) platform, guiding architecture decisions and engineering standards across deployments that serve PSAPs in more than 26 states. His technical depth in NG911 network architecture, combined with INDIGITAL's position as the originating architect of the nation's first large-scale public safety ESInet, makes him a uniquely qualified technical authority for statewide NG911 deployments.

Academic Background

MS, Agricultural Economics – Purdue University (1992–1997)

Professional Experience

Role	Organization	Description
Chief Technical Officer Current	INDIGITAL Telecom	Senior technical authority over INDIGITAL's ESInet platform, including SIP trunk interconnection design, Session Border Controller (SBC) configuration, and NENA i3-compliant network architecture supporting statewide deployments across more than 26 states. Directs technical standards for NGCS functional elements including NG-ALI/LDB, geo-based policy routing, Legacy Gateways, BCFs, and Conference Focus Agents.
IN911 Statewide Network (Indiana) Ongoing	INDIGITAL Telecom	Contributed to technical development and ongoing operations of Indiana's IN911 statewide ESInet, the first large-scale public safety IP network of its kind in the United States, now serving all primary PSAPs statewide.
Technology Consultant Prior	CCS Technology Group	Technology consulting spanning network design, SIP and VoIP protocols, wireless infrastructure, and Ethernet systems.
Security Technology Leader Prior	BearHill Security	Security technology leadership with focus on network hardening and physical security systems integration.

References: Available upon request.

Robert Brown

Chief Information Officer / Chief Security Officer | Proposal Role: **Security Lead**

Robert Brown has over 30 years in Information Technology and 35 plus years in Public Safety. Before working for INDIGITAL, he was part of the leadership team implementing Next Generation 911 services for the State of New Hampshire. He was a public sector representative to the National Public Safety Telecommunications Council as a voting member of the FCC's Task Force on Optimal PSAP Architecture and has been active in many other workgroups over the years.

Academic Background

Master of Science in Project Management – Granite State College

Bachelor of Science in Network Management – Granite State College

Professional Certifications

US Army Military Policeman

Professional Experience

Role	Organization	Description
Chief Information Officer / Chief Security Officer 2017–Present	INDIGITAL Telecom	Project managed the security SOC II type 1 and type 2 audits of the INDIGITAL NSOC and penetration testing of the INDIGITAL Texty platform. Leads cybersecurity compliance, information technology strategy, and security operations across the organization.
Project Manager – State of Vermont Recent	INDIGITAL Telecom	Executive oversight and project managed a statewide call delivery system, migration to NGCS, 911 Database services, and CHE.
Project Manager – Charleston County, SC Recent	INDIGITAL Telecom	Project managed the implementation of call delivery system, NGCS, text control services, and 911 Database services.
NG911 Implementation Leader Prior	State of New Hampshire	Part of the leadership team implementing Next Generation 911 services for the State of New Hampshire. Project management for renewal and upgrade of a statewide call delivery system, adding additional services, functionality, and resiliency.

References: Available upon request.

James Kinney

Chief Innovation Officer | Proposal Role: Technical Engineer / NG911 Software Architecture Lead

James Kinney is a public safety technology innovator and software engineering leader with a career defined by hands-on development of mission-critical NG911 systems. As Chief Innovation Officer at INDIGITAL, he directs the architecture, design, and engineering of the company's public safety solutions and software functional elements, with a particular focus on NG911/NGCS i3 standards, Unified Communications, and VoIP interworking. James leads INDIGITAL's internal R&D department, as well as two development teams spanning North America and Europe.

Academic Background

James A. Rhodes State College (2007–2009)

Professional Certifications

United States Army Veteran

Professional Experience

Role	Organization	Description
Chief Innovation Officer Current	INDIGITAL Telecom	Directs architecture, design, and engineering of INDIGITAL's public safety solutions and NGCS software functional elements. Leads internal R&D department and two development teams (North America and Europe).
Principal Architect – Texty (Text-FOR-911) Ongoing	INDIGITAL Telecom	Principal architect and lead developer of INDIGITAL's Texty platform, the first standards-based, operator-oriented SMS-to-911 solution deployed in the United States under J-STD-110. Serves hundreds of counties across multiple states.
NGCS Functional Elements In-House Development Lead Ongoing	INDIGITAL Telecom	Directed in-house design and development of NGCS software functional elements including NG-ALI (LDB) databases, geo-based and policy-based NG911 routing, Legacy Gateways, BCFs, Text Bridging, and Conference Focus Agents.
Three-Way Video Emergency Conference Lead (T-Mobile) Recent	INDIGITAL Telecom	Led engineering for INDIGITAL's successful test of the first-ever native three-way video emergency conference call, conducted in collaboration with T-Mobile.

References: Available upon request.

Sandi Stroud, ENP

Vice President, Public Safety | Proposal Role: **GIS and Location Services Lead / Proposal Manager**

Sandi C. Stroud, ENP, is a nationally credentialed emergency communications professional with a career built at the center of 911 network modernization, NG911 GIS standards, and statewide public safety program leadership. Sandi has served as 911 Program Manager for the State of Minnesota, directing the state's full transition from legacy to end-state NG911, and as Director of the Minnesota Geospatial Information Office (MnGeo), where she led development of the statewide NG911 GIS Roadmap.

Academic Background

BA, Urban Studies and Planning — California State University, Northridge (CSUN)

Professional Certifications

Emergency Number Professional (ENP) NENA

Professional Experience

Role	Organization	Description
Vice President, Public Safety Current	INDIGITAL Telecom	Leads public safety business development, GIS and location services strategy, and proposal development for statewide NG911 procurements nationwide.
911 Program Manager — State of Minnesota Prior	State of Minnesota	Directed full statewide transition from legacy 911 to end-state NG911, overseeing ESInet procurement, PSAP migrations, and interoperability across 87 counties.
Director, Minnesota Geospatial Information Office (MnGeo) Prior	State of Minnesota	Led development of the statewide NG911 GIS Roadmap, establishing the framework for GIS data governance and NG911 readiness across all jurisdictions.
FCC NG911 Compliance Leadership Current	INDIGITAL Telecom	Leads public-facing strategy and technical commentary on FCC Phase 2 NG911 migration rules, Location Validation Function (LVF) requirements, and NENA i3/CLDXF-US standards compliance.

References: Available upon request.

Steve Lantz

Vice President of Operations | Proposal Role: **Service Manager / NOC Operations Lead**

Steve Lantz has over 35 years in telecom, project management, and wireless carrier management. He was a regional manager at the deployment startup phase of a national provider, the PCS network, throughout the Midwest. At INDIGITAL, Steve manages operations of the NSOC, CHE Support, and field services. He has extensive involvement in the company's early projects for MSI, which utilize INDIGITAL software and core technologies.

Academic Background

Associate in electrical engineering – I.T.T. Technical Institute

Professional Certifications

IT Project Management Certificate – Global Knowledge

Professional Experience

Role	Organization	Description
Vice President of Operations 2016–Present	INDIGITAL Telecom	Manages operations of the National Service Operations Center (NSOC), CHE Support, and field services. Leads operational delivery for statewide and regional NG911 deployments.
Multi-State Deployment Leader Ongoing	INDIGITAL Telecom	Texas (Greater Harris County, Lubbock, multiple COGs), Maryland (Prince George's Co, Allegany Co, Howard Co, Garrett Co, Frederick Co), Alabama ANGEN v2.0–3.0, multiple Florida projects, 35 county deployments in Illinois, 85 county deployments in Michigan.
ESInet-to-ESInet Integration Lead – South Carolina Recent	INDIGITAL Telecom	Lead for the INDIGITAL ESInet to ComNet ESI-NET integration in South Carolina.
Regional Manager – PCS Network Prior	National Wireless Provider	Regional manager at the deployment startup phase of a national PCS network throughout the Midwest.

References: Available upon request.

Doug Kesser

Chief Revenue Officer | Proposal Role: **NG911 Sales and Business Development Lead**

Doug Kesser is a senior public safety technology executive with more than three decades of experience in telecommunications and emergency communications, spanning engineering, product development, and enterprise sales leadership. As Chief Revenue Officer at INDIGITAL, he brings a proven record of closing and growing major government and commercial NG911 contracts across the United States.

Academic Background

BS, Electrical Engineering – Penn State University

MBA – Rutgers University

Professional Certifications

United States Coast Guard Veteran (1988–1994)

Professional Experience

Role	Organization	Description
Chief Revenue Officer Current	INDIGITAL Telecom	Leads NG911 enterprise sales and revenue growth. Manages government and commercial NG911 contract capture across the United States.
Senior Solutions Sales Manager, NG911 Prior	Motorola Solutions	Led competitive positioning, state procurement, and long-cycle public safety sales for Motorola Solutions' NG911 portfolio.
Director, Public Safety / Safety & Security Technologies Prior	TeleCommunication Systems (TCS) / Comtech	Directed product roadmap and go-to-market strategy for emergency communications solutions. Supported pursuit and award of Pennsylvania statewide NG911 (\$175.1M), South Carolina statewide NG911, and Iowa statewide NG911 re-award.
Engineer / Researcher Prior	Telcordia Technologies / Bell Communications Research	Telecommunications engineering and systems architecture research. NASA Langley Summer Scholar (1997).

References: Available upon request.

Timothy J. Jenkins

Senior Operations Executive — Public Safety & Telecommunications | Proposal Role: **Executive Sponsor / Incoming COO**

Accomplished senior operations executive with a career spanning DATAMARK Technologies, Comtech, General Dynamics Information Technology (GDIT), West Safety Services/Intrado, and AT&T — marked by building strong operational delivery capabilities, customer loyalty, fully engaged teams of top industry talent, and delivering improvement on financial results. Thought leader in telecommunications operations, public safety, and Next Generation 9-1-1 with proven success in spearheading design and deployment of programs that optimize the customer experience. Developed and deployed the nation's first IP-based 9-1-1 call routing network and replicable implementation process.

Academic Background

MBA — The Ohio State University

BSEE, Electrical Engineering — Ohio Northern University

Professional Certifications

National Emergency Number Association (NENA)

Association for Public Communications Officials (APCO)

Past Board Member, Front Range Community College Foundation

Professional Experience

Role	Organization	Description
Chief Strategy Officer 2022–Present	DATAMARK Technologies, Columbus, OH	Fosters relationships with current and new clients and industry experts. Identifies industry trends, evaluates strategic partnerships and business development opportunities. Collaborates with company leadership and cross-functional teams to develop and implement strategic initiatives.
President, Terrestrial & Wireless Networks 2022–2024	Comtech Telecommunications, Seattle, WA	Provided leadership for all aspects of the Terrestrial & Wireless Networks segment — mobile location technologies, SMSC, wireless emergency alerts, 911 call routing, NG911 services, Text-to-911, and call management solutions. Staff: up to 836, Budget: \$220M+ revenue, \$40M+ EBITDA. Drove 2.6% YoY revenue improvement, 148.1% YoY operating income improvement, and \$6M+ cost reductions.

Role	Organization	Description
VP & GM, NG9-1-1 Programs 2019–2022	Comtech Telecommunications, Seattle, WA	Responsible for wireless, VoIP, and NG911 customer operations and growing the customer base through new contract awards. Staff: 140+, Budget: \$110M+ revenue. Full P&L ownership.
Vice President, 9-1-1 Solutions 2017–2019	General Dynamics IT (GDIT), Westwood, MA	Led the emerging NG9-1-1 solutions team. Deployed statewide i3-compliant NG9-1-1 solution implementing core services and hosted call handling to approximately 250 PSAPs in Massachusetts. Staff: 80+, Budget: \$50M+ revenue. Drove NOC improvements with ITIL-aligned processes.
SVP/GM Wireline Division; VP Delivery Ops 2000–2016	Intrado/West Safety Services, Longmont, CO	Full P&L responsibility across multiple VP and GM roles over 16 years. Won \$250M+ contract from competitor by leading negotiations with major telecom carrier. Delivered 1.5% and 2.2% YoY improvements in gross profit and operating income. Staff: 250+, Budget: \$90M+ revenue.
Director, 9-1-1 Operations 1985–2000	AT&T (SBC/Ameritech /Ohio Bell), Columbus, OH	Led 9-1-1 operational support for the five-state AT&T Midwest region including planning, implementation, ongoing customer service, and data integrity for 860 PSAPs. Staff: 70+. Migrated three unique platforms into a single platform and standardized all support processes.

References: Available upon request.