

**NATIONAL CAPITAL REGION (NCR)**

**REQUEST FOR PROPOSALS**

**NEXT GENERATION CORE SERVICES (NGCS) SOLUTION  
For  
Northern Virginia and Suburban Maryland Counties**

**August 26, 2016**

Fairfax County is accepting proposals from qualified Respondents to provide a NGCS solution.

## TABLE OF CONTENTS

<b>1. BACKGROUND AND PROJECT SCOPE.....</b>	<b>1</b>
<b>2. OBJECTIVES.....</b>	<b>3</b>
2.1. EXPECTATION.....	3
2.2. RESPONDENT PROFILE .....	3
<b>3. GENERAL REQUIREMENTS.....</b>	<b>4</b>
3.1. PROJECT KNOWLEDGE .....	4
3.1.1. <i>Responses to Each Requirement</i> .....	4
3.2. RESPONDENT VISION OF NG9-1-1 .....	5
3.3. SINGLE POINT OF CONTACT .....	5
3.4. INFORMATION PROVIDED BY THE RESPONDENT.....	5
3.5. COMPLIANCE SUMMARY .....	6
<b>4. TECHNICAL REQUIREMENTS.....</b>	<b>6</b>
4.1. CAPACITY .....	6
4.2. STANDARDS .....	6
4.3. NETWORK.....	8
4.4. INTERCONNECTION TO LEGACY SELECTIVE ROUTERS.....	10
4.5. INTERCONNECTION TO OTHER ESINETS .....	11
4.6. INTEROPERABILITY WITH STATE POLICE, MILITARY BASES, AND OTHER FEDERAL ENTITIES.....	12
4.7. DATA CENTERS .....	12
4.7.1. <i>Data Center Locations</i> .....	13
4.7.2. <i>Data Center Requirements</i> .....	13
4.7.3. <i>Cabinets and Power Distribution</i> .....	14
4.7.4. <i>Support Maintenance</i> .....	15
4.8. SECURITY .....	15
4.8.1. <i>Physical Security</i> .....	17
4.9. NETWORK OPERATIONS CENTER (NOC)/SECURITY OPERATIONS CENTER (SOC) .....	18
4.9.1. <i>Security Monitoring and Management</i> .....	18
4.9.2. <i>Incident Management System</i> .....	19
4.9.3. <i>Change Management System</i> .....	20
4.9.4. <i>Management Software</i> .....	20
4.9.5. <i>Network and System Event Logging</i> .....	21
4.9.6. <i>Physical Access Monitoring and Management</i> .....	22
4.9.7. <i>Access to Technical Staff</i> .....	22
4.9.8. <i>Notification</i> .....	23
4.9.9. <i>Escalation Procedures</i> .....	23
4.9.10. <i>Change Management Processes and Procedures</i> .....	23
4.9.11. <i>Statement on Standards for Attestation Engagement Number 16</i> .....	24
4.9.12. <i>Configuration Backup and Restoration</i> .....	24
4.9.13. <i>Third-Party Management</i> .....	25
4.9.14. <i>Operational Scenarios</i> .....	26
4.10. NG9-1-1 CORE SERVICES (NGCS) ELEMENTS .....	27
4.10.1. <i>Legacy Network Gateway (LNG)</i> .....	27
4.10.2. <i>Legacy PSAP Gateway (LPG)</i> .....	30

4.10.3.	<i>Border Control Function (BCF)</i>	32
4.10.4.	<i>Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)</i>	36
4.10.5.	<i>Emergency Call Routing Function (ECRF)</i>	40
4.10.6.	<i>Location Validation Function (LVF)</i>	43
4.10.7.	<i>Spatial Interface (SI)</i>	45
4.10.8.	<i>Location Database (LDB)</i>	46
4.10.9.	<i>Discrepancy Reporting</i>	48
4.10.10.	<i>Event Logging and Management Information System (MIS)</i>	48
4.10.11.	<i>Network Time Protocol (NTP) &amp; Time Source</i>	51
4.10.12.	<i>NG9-1-1 Applications and Alarm Integration</i>	51
4.10.13.	<i>Message Session Relay Protocol (MSRP) Text Integration</i>	52
4.11.	<b>SERVICE LEVEL AGREEMENTS (SLA)</b>	52
4.11.1.	<i>System Capacities and Performance</i>	52
4.11.2.	<i>System Performance</i>	53
4.11.3.	<i>SLAs for Incident Management</i>	56
4.11.4.	<i>Outage Notification and Reason for Outage (RFO) Report</i>	56
4.11.5.	<i>SLA Reporting</i>	58
4.11.6.	<i>SLA Violations</i>	58
4.11.7.	<i>Incident Severity Level 1 and 2 Violation Damages</i>	59
4.12.	<b>PSAP INTERFACES AND BACKROOM EQUIPMENT REQUIREMENTS</b>	59
5.	<b>MIGRATION PLAN OPTIONS</b>	62
6.	<b>PROJECT MANAGEMENT AND ON-GOING CLIENT MANAGEMENT SERVICES</b>	63
7.	<b>TRAINING</b>	65
8.	<b>SERVICE, REPAIR AND ADVANCE REPLACEMENT</b>	65
9.	<b>SOFTWARE RELEASE POLICY</b>	66
9.1.	<i>SCHEDULED RELEASES</i>	66
9.2.	<i>MAINTENANCE RELEASES</i>	66
10.	<b>DOCUMENTATION</b>	67
	<b>ATTACHMENT A: NCR PSAP DATA FOR PROPOSED ESINET AND NGCS</b>	699
	<b>ATTACHMENT B: NCR GIS DATA MODEL</b>	73
	<b>ATTACHMENT C: REQUIREMENTS COMPLIANCE SUMMARY</b>	78
	<b>ATTACHMENT D: SAMPLE OF REQUIRED 10-DIGIT TRANSFERS</b>	85

## 1. BACKGROUND AND PROJECT SCOPE

The National Capital Region (NCR)<sup>1</sup> is preparing for a migration from legacy, circuit-switched 9-1-1 with limited interoperability to a Next Generation 9-1-1 (NG9-1-1) regional system built on a standards-based, Emergency Services Internet Protocol (IP) network (ESInet) that will enable seamless interoperability across the region. This request for proposals (RFP) is the first step in progressing toward the NCR's end vision of regional interoperability.

The NCR has been working collaboratively to ensure a smooth migration to the Next Generation platform. The establishment of the 9-1-1 Directors Committee under the Metropolitan Washington Council of Governments (MWCOC) has brought together regional 9-1-1 stakeholders to work across jurisdictional lines toward a reliable and redundant regional solution. Recently, the committee established an NG9-1-1 working group to assess the technical and operational needs of the region.

This Next Generation Core Services (NGCS) and ESInet procurement for the NCR consists of 14 primary, 9 secondary, and 10 backup public safety answering points (PSAPs) residing in the State of Maryland and the Commonwealth of Virginia. The counties and cities included within the NCR that are participating in this procurement may be seen in Figure 1, below. A complete list of participating NCR PSAPs may be found in Attachment A. Each jurisdiction will procure its service through this RFP and contract with the Contractor independently.

Respondents may notice that two of the NCR's jurisdictions are not participating in this procurement. The District of Columbia (D.C.) Office of Unified Communications (OUC) is in the process of independently deploying, and Loudoun County Emergency Communications Center (ECC) has independently deployed, NG9-1-1 call-routing services with West Safety Services (West). Specifically, both jurisdictions have independently deployed, or are in the process of deploying, IP selective routing (IPSR) services, and it is anticipated that both eventually will migrate to geospatial routing using National Emergency Number Association (NENA) i3 protocols during the initial term of the NCR's NGCS services. The NCR requires interoperability with these two neighboring jurisdictions on Day 1.

---

<sup>1</sup> The NCR region, in the context of this RFP, includes the following Virginia, Maryland, and District of Columbia jurisdictions and municipalities included with those jurisdictions: (1) The City of Alexandria, VA (2) Arlington County, VA, (3) Calvert County, MD (4) Charles County, MD, (5) the District of Columbia, (6) Fairfax County, VA, (7) Fauquier County, VA, (8) Frederick County, MD, (9) Loudoun County, VA, (10) Montgomery County, MD, (11) Prince George's County, MD, (12) Prince William County, VA, (13) St. Mary's County, MD, and (14) Stafford County, VA. Some federal planning programs may list different jurisdictions in their definition of the NCR.

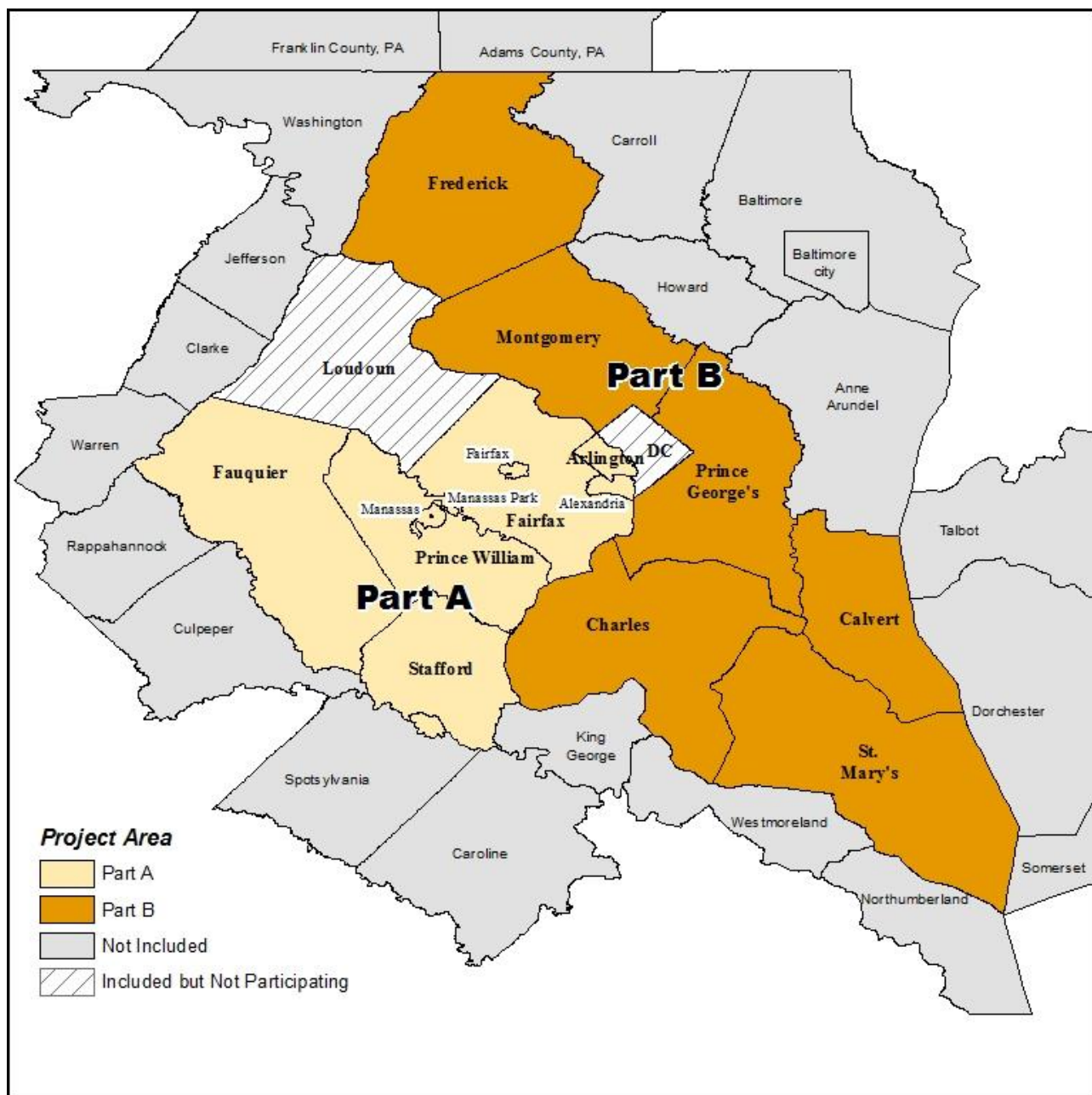


Figure 1: NCR Map

The NCR understands that other NG9-1-1 components and GIS data development must be implemented prior to, or in conjunction with, the NGCS. The NCR is seeking to procure and deploy a transitional NGCS solution with managed ESInet services. This transitional solution should align with NENA-INF-008.2-2014, providing for geospatial routing of calls with the implementation of legacy network gateways (LNG), border control function (BCF), emergency service routing proxy (ESRP), policy routing function (PRF), emergency call routing function (ECRF), location validation function (LVF), spatial interface (SI) and location database (LDB).

In January 2016, the NCR PSAPs initiated a project to develop a common GIS data set across the region. Individual jurisdictions are developing their boundaries and street centerline data, which is being uploaded to a common database for quality assurance (QA) and quality check (QC) analysis. The disparate data sets then will be coalesced into a single dataset and loaded into a test ECRF and LVF. The project will conclude in May 2018, at which time the data will be capable of meeting the data requirements for all fields marked as required in Attachment B of NENA 08-003, and meet all spatial audits as described in Section 4.3 of NENA 02-014. A copy of the NCR's GIS data model may be viewed in Attachment B.

The NCR PSAPs have individually deployed, or will be individually deploying, NG9-1-1 call-handling systems to interface with the NGCS. In some cases, secondary PSAPs may require the Contractor to deploy a legacy PSAP gateway (LPG) to interface with its legacy E9-1-1 call-handling solution. New call-handling equipment is not in the scope of this procurement, and proposals that include call-handling solutions may be disqualified.

## **2. OBJECTIVES**

### **2.1. EXPECTATION**

The NCR desires that NGCS provide the call-routing intelligence required by a next-generation system. The functional elements include transitional elements as well as NGCS, including, but not limited to, the following:

- Legacy Network Gateway (LNG)
- Legacy Public Safety Answering Point (PSAP) Gateway (LPG)
- Border Control Function (BCF)
- Emergency Services Routing Proxy (ESRP)
- Policy Routing Function (PRF)
- Emergency Call Routing Function (ECRF)
- Location Validation Function (LVF)
- Location Database (LDB)
- Spatial Interface (SI)
- PSAP Interfaces
- Discrepancy Reporting
- Event Logging
- Time Server

### **2.2. RESPONDENT PROFILE**

Each Respondent shall provide a brief description of its company and experience with similar projects. As part of this profile, each Respondent also shall list business partner(s) for this proposal, with an explanation of why its business partner(s) was chosen and its experience with similar projects.

### 3. GENERAL REQUIREMENTS

#### 3.1. PROJECT KNOWLEDGE

##### 3.1.1. Responses to Each Requirement

The responses to each requirement described in this RFP must include one of the following:

**Understood:** The Respondent understands the statement without question or providing clarification.

**Complies:** The Respondent proposal complies with the RFP requirements and the products/services are included in the base price, are currently developed, and are available for implementation (i.e., must be generally available).

**Complies Partially:** The Respondent proposal addresses the RFP requirements through another method that is currently developed and is available for implementation (i.e., must be generally available), or the solution complies with some, but not all of the requirements. Respondent is responsible for clearly explaining how its proposed solution does not fully comply.

**Complies with Future Capability:** The RFP requirements will be met with a capability delivered at a future date. This response must include a calendar quarter and year that the requirement will be met with a generally available product or service at no additional cost.

**Does Not Comply:** The Respondent proposal does not/cannot meet the specific RFP requirement.

1. Below each requirement will be either one (Understood) check box or four check boxes (Complies, Complies Partially, Complies with Future Capability, Does Not Comply). Respondent must respond by placing an "X" in only **one** check box per stated requirement. Failure to complete this process properly will be treated the same as "Did Not Answer."

☐ Understood

2. A response and description to each requirement is required. Do **not** underestimate the importance of providing details. The details should be sufficient to properly convey Respondent's intentions, but should not be verbose in nature. Marketing materials are not considered appropriate in-line responses. Respondent may attach marketing materials as separate, supplemental documents, but details are still required to support the answer.

☐ Understood

3. Respondent shall not refer to other sections as a response. Even if the response is an exact duplicate of a previous response, the details must be provided in the same paragraph as the requirement. Respondent must not include pricing information in its description, and must not refer the reader to pricing; note that the NCR's evaluation team(s) members will not have access to pricing information.

☐ Understood

### **3.2. RESPONDENT VISION OF NG9-1-1**

The NCR is interested in retaining the Respondent that understands and can clearly demonstrate alignment with the industry's evolution to NENA NGCS solutions. Each Respondent shall describe its vision of NG9-1-1 and how it aligns with NENA's vision.

Also noteworthy would be items such as position papers or partnerships/alliances intended to further the vision of the NGCS. All proprietary documents must be clearly marked.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

### **3.3. SINGLE POINT OF CONTACT**

The successful Respondent shall be the Contractor of record and serve as the NCR's single point of contact ("Prime") for proposals and any contract that may result from this RFP. The Prime is responsible for any partners or subcontractors.

☐ Understood

### **3.4. INFORMATION PROVIDED BY THE RESPONDENT**

Respondent is solely responsible for conducting its own independent research, due diligence or other work necessary for the preparation of responses, negotiation of contracts and the subsequent delivery of services pursuant to any contract resulting from this RFP. NCR takes no responsibility for the completeness or the accuracy of any information presented in this RFP, or otherwise distributed or made available during this selection process or during the term of any subsequent contract.

☐ Understood



### 3.5. COMPLIANCE SUMMARY

Respondent shall state its compliance in the summary table provided in Attachment C, as depicted below:

☐ Understood

## 4. TECHNICAL REQUIREMENTS

### 4.1. CAPACITY

1. All IP network components, physical network segments, and NGCS elements shall support each PSAP's current call-handling capacity, plus 25 percent growth over the life of the initial contract. All networks and NGCS elements shall be designed with no single points of failure. All equipment shall be new and of current manufacture. Used, refurbished, or end-of-life equipment shall not be used.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

2. If the Respondent's solution is rate limited, Respondent shall state the maximum number of calls per second that the proposed solution can sustain. Respondent also should specifically address how multimedia and text calls will affect call-handling capacity.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

### 4.2. STANDARDS

The NCR seeks a standards-based solution that complies with all applicable NENA, Association of Public-Safety Communications Officials (APCO), American National Standards Institute (ANSI), and Internet Engineering Task Force (IETF) standards. Proprietary solutions or solutions with limited compliance with industry-standards may be disqualified if it is determined that the solution will not immediately achieve the NCR's goal of interoperability throughout the region, with

neighboring legacy selective routers, and with future neighboring ESI-nets.

As industry standards evolve, the Contractor's solution shall continue to comply with industry standards. Specifically, the Contractor's solution shall comply with new NGCS and ESI-net industry standards within 12 months of ratification of applicable industry standards. This applies to current and future revisions of the following list of standards, and the supporting standards referenced within each standard. As solution updates are made to maintain industry standards compliance, the solution shall not abandon services or feature functionality in place at the time of the solution upgrade. Applicable industry NG9-1-1 standards and informational documents include, but are not limited to:

- NENA 08-003, *Detailed Functional and Interface Specification for the NENA i3 Solution*, Stage 3 Version 1, and its successors
- NENA 75-001, *Security for Next Generation 9-1-1 Standard (NG-SEC)*, and its successors
- NENA 08-506, *Emergency Services IP Network Design for NG9-1-1 Information Document*, Version 1, and its successors
- NENA-STA-003.1.1-2014, *NENA Standard for NG9-1-1 Policy Routing Rules*, and its successors
- NENA-REQ-002.1-2016, *NENA Next Generation 9-1-1 Data Management Requirements*, and its successors
- NENA-STA-004.1.1-2014, *NENA Next Generation 9-1-1 United States Civic Location Data Exchange Format (CLDXF)*, and its successors
- NENA/APCO-INF-005, *NENA/APCO Emergency Incident Data Document (EIDD)*, to be replaced by its eventual ANSI document
- NENA-STA-006.1-201x, *NENA GIS Data Model for NG9-1-1 (Draft)*
- IETF base IP protocols
- IETF IP-routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF)
- IETF session and media protocols such as Session Initiation Protocol (SIP), Session Description Protocol (SDP), Message Session Relay Protocol (MSRP), and Real-Time Transport Protocol (RTP)
- IETF protocols such as Location-to-Service Translation (LoST), HTTP-Enabled Location Delivery (HELD), and Presence Information Data Format Location Object (PIDF-LO)

Respondent shall reveal any use of proprietary standards or protocols in its proposed solution, or state that it fully complies with this requirement. Any limitations, whether technological or philosophical, shall be disclosed in the response.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

### 4.3. NETWORK

1. Respondent must include in its proposal the fully functional ESInet services capable of supporting the NCR's primary, backup, and secondary locations, including interconnectivity with West, the ESInet provider to the District of Columbia OUC and the Loudoun County ECC. Contractor will have to interconnect with other regional and state-level ESInets in the future, at which time scope and costs will be assessed.

☐ Understood

2. As defined in NENA 08-003, "An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all Public Safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including but not limited to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based internetwork (network of networks)."

The NCR's desire is to implement a redundant, resilient, public safety-grade (99.999 percent uptime), managed, IP-based ESInet. Contractor shall design such a network to provide the infrastructure for NENA i3 core services and processes (NGCS), while interconnecting and providing interoperability for all of the NCR's primary, backup, and secondary locations as shown in Attachment A.

☐ Understood

3. The network shall be designed with diverse entrances (e.g., "east-west" entrances) into each facility that is a part of the NCR ESInet, including data centers, PSAPs, and other locations. Primary and redundant links shall not share common routes, trenches, or poles. If facility construction is required, Respondent shall so indicate. In the event that this is not possible at a given location, Respondent shall indicate how it intends to provide redundant and resilient connectivity to that location. The NCR is open to proposals that provide non-terrestrial transport if priced as an option.

☐ Understood

4. All network equipment shall be new and of current manufacture. All servers, systems, routers, switches, and other network equipment shall support IPv4 and IPv6, and be capable of running dual protocol stacks.

☐ Understood

5. The NCR's view of the network shall be at Layer 3 of the International Organization for Standardization (ISO) model, i.e., IP packets are routable between any two points on the ESInet. The network shall comply with Institute of Electrical and Electronics Engineers (IEEE) 802.3 Ethernet standards, as well as the Internet Engineering Task Force (IETF) requests for comments (RFC).

☐ Understood

6. Internal network routing shall be accomplished through use of the Open Shortest Path First (OSPF) protocol, as defined in RFC 2328 and RFC 5340. External network routing, such as that to service providers and other ESInets, shall be through the use of the Border Gateway Protocol (BGP) as defined in IETF RFC 4271. All routing protocols shall implement authentication between neighboring routers. Other standards-based protocols may be considered by the NCR, but the use of proprietary routing protocols is prohibited.

☐ Understood

7. Resiliency, or fast failover, may be achieved through the use of the Bidirectional Forwarding Detection (BFD) protocol as defined in IETF RFC 5880 and RFC 5881, or other standards-based, non-proprietary methods approved by the NCR.

☐ Understood

8. All routers and switches must support multicast routing and switching. The applicable base protocols are Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM). These protocols handle the routing of join and leave requests for the multicast streams across both local and wide-area networks. IGMP version 3 (IGMPv3) is the most current version and is defined in RFC 3376. This RFC was amended by RFC 4604, which added Multicast Listener Discovery (MLDv2), which provides the equivalent functionality for IPv6. There are four varieties of PIM: sparse mode (RFC 4601), dense mode (RFC 3973), bidirectional mode (RFC 5015), and source-specific mode (RFC 3569).

☐ Understood

9. The network equipment shall support Quality of Service (QoS) marking for prioritizing traffic in the network using the Differentiated Services Code Point (DSCP) protocol. While the network can change DSCP values through rules, the values typically are set by the system or functional element that originates the traffic. Network routers and switches shall not be configured in such a manner as to change DSCP values set by originating functional elements.

☐ Understood

10. The proposed ESInet shall be private, robust, scalable, secure, diverse, redundant, and sustainable. Respondent shall propose a network solution for all sites listed in Attachment A.

☐ Understood

11. Contractor is responsible for any third-party certification fees.

☐ Understood

12. Respondent shall describe how its proposed solution meets each of the requirements outlined in Section 4.3.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

13. Using the information provided in Attachment A, Respondent shall provide the proposed bandwidth for each PSAP. The bandwidth calculations for PSAPs served by hosted call-handling systems should be included in the host site's bandwidth. If the PSAP's current trunking, position count and call volume places its proposed bandwidth within 80 percent of being fully utilized, then Respondent shall provide an indication of the next-higher tier of bandwidth and include a corresponding line item in the optional pricing table.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

#### **4.4. INTERCONNECTION TO LEGACY SELECTIVE ROUTERS**

1. Contractor must provide redundant, resilient Legacy Network Gateways (LNGs) with Legacy Selective Router Gateway (LSRG) functionality to allow the legacy selective routers to transfer calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information to the NCR's NGCS and vice versa. LSRG functionality shall allow for legacy PSAPs served by legacy selective routers to serve as the abandonment route for NCR PSAPs served by the Contractor's ESInet and NGCS.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall explain how it has worked with Legacy Selective Router providers with similar solutions on similar projects, and shall provide specific plans for working with the NCR's legacy 9-1-1 service provider, Verizon.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.5. INTERCONNECTION TO OTHER ESINETS**

Two of the NCR's jurisdictions, D.C. and Loudoun County, have deployed, or are in the process of deploying, NG9-1-1 call-routing services from West. Specifically, both jurisdictions have independently deployed, or are in the process of deploying, IPSR services and it is anticipated that both eventually will migrate to geospatial routing using NENA i3 protocols during the initial term of the NCR's NGCS services. Similar to the need for legacy selective routers to interoperate, the NCR requires interoperability on Day 1 between neighboring ESInets that may provide IPSR services or NGCS to their PSAPs. Respondent shall describe how its proposed solution will seamlessly interwork with West and other neighboring ESInets that serve their clients with IPSR and/or NGCS. Respondents shall assume that interconnection with West will require multiprotocol label switching (MPLS) handoff at West's Miami, Florida, and Englewood, Colorado, data centers with thorough non-live interoperability testing. Respondents shall provide costs for interoperating with D.C. and Loudoun County, as expressed as a One Time Fee in the Cost Proposal.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.6. INTEROPERABILITY WITH STATE POLICE, MILITARY BASES, AND OTHER FEDERAL ENTITIES**

1. The NCR contains several military bases and other federal institutions that have special security and first responder operations. In many cases, the federal entity has Centralized Automated Message Accounting (CAMA) trunks from the legacy selective routers and is able to bid ALI, providing for the ability to receive call transfers with ANI and ALI information. Meanwhile, state police PSAPs send and receive all transfers via 10-digit lines without ANI and ALI information. A sample of required 10-digit transfers may be viewed in Attachment D.

Respondent shall describe how it can provide the same or improved capability for these special secondary PSAPs. Optional pricing is requested for potential future addition of these entities. Respondents shall assume that these sites have legacy CPE, fewer than 10 CAMA trunks, and fewer than 10 positions.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.7. DATA CENTERS**

The network and NGCS are provided by an array of firewalls, routers, gateways, and servers. The servers may include Storage Area Network (SAN) or Network Attached Storage (NAS) devices, which are high-capacity, redundant, resilient hard-disk storage systems. These are the types of devices that will be housed in multiple regional data centers. If the decision is made to co-locate a hosted call-handling system in these centers, those systems also will be comprised of similar equipment. These devices typically are mounted in four-post lockable cabinets, rather than open racks.

Respondent shall provide descriptions of previous data center implementations for similar solutions, along with specific details for the Respondent-recommended solution.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### 4.7.1. Data Center Locations

1. The host data centers must provide sufficient geodiversity to provide physical diversity in case of a widespread disaster. The NCR desires that at least one of the proposed data centers be within a 50 mile radius of the NCR footprint, but it is not required. The proposed solution should include at least two data center locations for hosting NGCS. Additional data centers may be required for hosting LNGs serving the region. A value proposition for implementing or not implementing a third data center, which could be taken off-line for testing software, is desirable. Each data center shall be able to support 100 percent of the expected 9-1-1 communications, in a failover mode.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

2. The Respondent shall provide examples of its implementation of NGCS in multiple data centers similar to the proposed solutions. Details, including sample drawings, shall be provided supporting the proposed data center solution.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

#### 4.7.2. Data Center Requirements

The data centers should meet Tier 4 design standards as detailed in Telecommunications Industry Association (TIA) 942, Data Center Standards, but at a minimum must meet Tier 3 standards to be considered as a viable location. Design standards include, but are not limited to the following:

- Redundant commercial power (supplied from separate grids if possible)
- Redundant backup generators
- Redundant uninterruptible power supplies (UPS)
- Redundant heating, ventilation, and air-conditioning (HVAC) systems
- Fire suppression systems
- Physical access security
- Physically separate communication service provider entry points



American National Standards Institute (ANSI)/TIA-606-B governs the operation and administration of data centers. It covers such topics as space and equipment labeling, cable labeling and color coding, cable classes, and grounding and bonding. This standard lays out a complete marking standard for data centers using a 2-foot grid of the room and designating each square with letters and numbers starting at AA01. All cabinets, racks, patch panels, and devices within said cabinets and racks should be identified and labeled front and rear.

All NCR systems and network equipment shall be housed either in a locked and monitored cage within a secure data center, or in its own locked and monitored room within a secure data center. Simply providing space in a common area is not acceptable.

The Respondent shall provide detail regarding how its proposed solution meets these requirements. These details will include specifics regarding certifications that confirm these requirements are met.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.7.3. Cabinets and Power Distribution**

1. Cabinets shall be fully enclosed and lockable. The front and rear doors may be vented or solid. If the doors are solid, adequate ventilation must be provided to remove the heat from the cabinet.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Many options are available for power distribution units (PDUs) that provide power inside the cabinets. At a minimum, the PDU should be remotely manageable via the Simple Network Management Protocol (SNMP), and provide load information back to the network management system. Given the wide geographic dispersion of the data centers, it is advisable to consider PDUs that have individually controllable outlets, in order to remotely power-cycle equipment that otherwise may be unresponsive. This ability should be coupled with remotely accessible console servers to allow console access into devices in the data centers.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### 4.7.4. Support Maintenance

1. Respondent shall describe in detail its 24 x 7 x 365 maintenance support for the life of the service-based solution. Respondent shall describe its understanding of public safety maintenance windows and associated notification processes. Respondent shall describe its problem and change management processes and supporting systems, and its adherence to best practices, such as those described in Information Technology Infrastructure Library (ITIL) version 3.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### 4.8. SECURITY

1. The security requirements apply equally to all elements of the system requested in this RFP, including but not limited to the following:
  - Data centers
  - PSAPs
  - ESInets
  - NGCS elements
  - Other facilities housing any element or device that is a part of the overall system

The proposed solution's security program is required to utilize the latest NENA specifications and incorporate the intentions of the Communications Security, Reliability and Interoperability Council (CSRIC) "Best Practices."<sup>2</sup> All applicable rules and regulations of the Federal Communications Commission (FCC), in addition to those specified herein, shall apply.

---

<sup>2</sup> As found at <http://transition.fcc.gov/pshs/advisory/csric>; WG1A, WG2A, WG2B, WG4A, WG4B, WG4C, WG5A, WG6, WG7 and WG8

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall provide a compliance matrix, as outlined in NENA 75-502, NENA NG-SEC Audit Checklist, which identifies whether its proposed solution Complies (C), Complies Partially (CP), Complies with Future Capability (CFC) or Does Not Comply (DNC) to the identified requirement(s) for each audit question, using the instructions provided in Section 3 of NENA 75-502.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. Respondent shall describe its capabilities to provide predictive analysis and modeling to combat security threats.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. The Respondent's proposed solution shall provide a process so that devices and carriers outside the ESInet shall not have credentials, per NENA-08-003 or its successor document. The Respondent shall provide details regarding how its proposed solution ensures that devices and carriers outside the ESInet are not provided credentials.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. Contractor shall allow for annual third-party security audits at the request and cost of the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

6. A comprehensive security plan is a critical component of the NCR's NGCS solution. The Respondent shall describe its security plan, monitoring processes, and incident response processes.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.8.1. Physical Security**

1. All facilities housing components of the NCR ESInet and NGCS shall have security and access control systems that ensure only duly authorized individuals can access the areas housing the NCR's systems and network equipment. Any workstations or other PSAP equipment connected to the ESInet shall be housed in secured, access-controlled areas. Any devices, power distribution, and cross-connect panels feeding the cages or rooms housing the NCR's systems shall be similarly protected.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Contractor, upon request, shall furnish monthly reports on physical access to the NCR ESInet and NGCS facilities, including failed attempts.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9. NETWORK OPERATIONS CENTER (NOC)/SECURITY OPERATIONS CENTER (SOC)**

1. All components of the proposed solution shall be monitored 24 x 7 x 365 by a centralized Network Operations Center (NOC) and Security Operations Center (SOC). These functions may be in separate facilities or combined in a single facility.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall describe its NOC/SOC operations model, continuity of operations plan (COOP), problem and change management systems, reporting systems, escalation plan, and conformance with best practices for service delivery management.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

##### **4.9.1. Security Monitoring and Management**

1. The Contractor's security management solution shall control access to network resources according to public safety network security guidelines to prevent sabotage (intentional or unintentional) and the compromise of sensitive information. Security management shall use public safety network security standards to monitor users logging into network resources and refuse access to those who enter inappropriate access codes. The proposed IP-enabled network shall support standard security policies that may include the use of firewall rules, access control lists (ACLs), virtual local-area networks (VLANs), virtual private networks (VPNs), and Secure Sockets Layer (SSL) protocols to control network traffic and access. The systems and servers shall support the use of software to detect and mitigate viruses, malware, and other attack vectors.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Furthermore, any system that connects to an IP-enabled network shall be required to comply with applicable standards, including security standards, and demonstrate compliance through an initial and recurring audit.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. Contractor shall provide security reports on a monthly basis, including, but not limited to: incidents and incident response, and updates or changes to security systems and software.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. Respondent shall provide details concerning how it provides security monitoring and management for similar solutions. Respondent shall provide details, including drawings, which explain how its proposed solution meets or exceeds the above requirements.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.2. Incident Management System**

The Contractor's incident management system shall log all support requests, both from users and those automatically generated. The Respondent shall provide examples of monthly reports detailing tickets opened, resolved, and pending.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.3. Change Management System**

1. The change management system shall log all change requests, both from users and those automatically generated. The system shall interface with the incident management system for correlation of changes and outages. The Respondent shall describe its change management process and its ability to provide the NCR Program Manager with the ability to review proposed change requests and the client approval process. The Contractor shall provide monthly reports detailing change tickets opened, resolved, and pending.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The Respondent shall provide detailed descriptions of any other tools it intends to use in order to provide access to the change management system, such as Web portals and client software.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.4. Management Software**

1. Much is said about SNMP in network and server management discussions, but it is only the underlying protocol for transporting management information across the network. Software packages are widely available for capturing, analyzing, and reporting the network's health based on the SNMP traffic it receives. Several commercial packages are available, such as SolarWinds, Monolith, and OpenView, as well as many full-featured open source packages, such as OpenNMS, Nagios, and Network Management Information System (NMIS).

Respondent shall provide the name and description of the management software it has implemented, including all functional modules associated with it (e.g., reporting, backup, and IP address management).

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall provide a detailed explanation and associated drawings explaining how its proposed solution interworks with all of the various elements and services of the total NCR NG9-1-1 solution, and meets or exceeds the above requirements.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.5. Network and System Event Logging**

1. The IP network and the NGCS shall allow historical tracking of network and system events, as well as event resolution. This is for logging errors and statistical information related to the health of the network and the NGCS.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. It is preferable that this system be part of, or interfaced with, the various Contractor and supplier trouble ticketing systems, or contain cross-reference abilities. Contractor shall maintain historical information for the term of the contract, and provide copies of the data to the NCR at the end of the contract.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:



3. Respondent shall provide a detailed explanation and associated drawings explaining its processes and procedures for interfacing with the Respondent and supplier solutions. Respondent shall provide details regarding how its proposed solution meets or exceeds the above requirements.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.6. Physical Access Monitoring and Management**

1. Contractor shall track and log all attempts to access the cabinets, data center cage, or rooms housing the NGCS components serving the NCR. Reports may be requested and shall be made available for review as part of problem management reporting.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall provide a detailed explanation of its processes and procedures for logging physical access to the NGCS components, and how it generates the required reports.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.7. Access to Technical Staff**

The Contractor shall detail the procedures by which it communicates with technical personnel from participating suppliers and the NCR entities. The Respondent shall specify the level of assistance expected from such technical personnel to resolve service-related issues. Security personnel are expected to recommend solutions to various malicious network activities. Respondent shall provide a detailed explanation and associated graphical presentations explaining how its proposed solution meets or exceeds the above requirements.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.8. Notification**

Respondent shall specify how its NOC informs participating jurisdictions or their designee of problems with the network, scheduled outages, and upgrades. Tickets related to the services delivered to Contractor suppliers shall be forwarded automatically. Notification shall be provided via multiple communications means to NCR entities. Entities requiring notification may change, depending on the alarm or incident. Respondent shall provide a detailed explanation explaining how its proposed solution meets or exceeds the above requirements.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.9. Escalation Procedures**

Respondent shall outline a detailed jurisdiction-level escalation process to be used during incidents that affect service, particularly those that result in critical service outages. Respondent shall describe how discrepancies in the perception of service level agreement (SLA) incident levels may be escalated and addressed. It is preferable that these procedures be maintained and accessible via an online portal. This notification shall be integrated with the notification processes described above, based on alarm or incident. Respondent shall provide a detailed explanation explaining how its proposed solution meets or exceeds the above requirements.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.10. Change Management Processes and Procedures**

Respondent shall outline a detailed change management process. The ITIL change management standards are preferred, but not required. Respondent shall include explanation of its fault, configuration, accounting, performance, and security (FCAPS) procedures. Respondent shall provide a detailed explanation explaining how its proposed solution meets or exceeds the requirements for the ITIL and FCAPS processes.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.11. Statement on Standards for Attestation Engagement Number 16**

Contractor shall demonstrate compliance with the Statement on Standards for Attestation Engagements Number 16 (SSAE 16). This replaced the Statement on Accounting Standards 70 (SAS 70) in 2011. The applicable report from an SSAE 16 engagement is the Service Organization Controls 1 (SOC 1) report.

Respondent shall provide a detailed explanation of how it has complied with SSAE 16 for similar solutions and how this would be implemented with the NCR NG9-1-1 implementation. The Respondent shall provide with its detailed explanation a graphical representation explaining how its proposed solution meets or exceeds the above requirement.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.9.12. Configuration Backup and Restoration**

The Contractor and various suppliers shall deploy the capability to automatically or routinely back up configuration data, and define the conditions under which it will restore the configuration of network elements, such as routers or switches, and the process it will use should the need arise.

In addition to automatic, regular backups, Contractor and the various suppliers shall describe their ability to perform on-demand backups, such as at the end of a successful configuration change.

The Respondent shall provide a detailed explanation and any associated drawings explaining how its proposed processes and procedures provide the ability to manage these configuration backup

and restoration processes in a manner that has no negative impact on the total NCR NG9-1-1 solution.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### 4.9.13. Third-Party Management

The NCR desires the optimum value provided by best-of-class products and services integrated as part of its total NG9-1-1 solution. This may present a situation where no single manufacturer or supplier can provide a public safety-grade unified NOC/SOC accountability for all components, products and services that comprise the NCR's total NG9-1-1 solution. Consequently, the NCR may find it beneficial to have a third party provide that overarching NOC/SOC service.

A third-party NOC/SOC provider may be responsible for functioning as an umbrella for monitoring all of the Contractor's products and services, including collaboration with the Contractor's NOC/SOC. To facilitate that capability, the third-party NOC/SOC must have a view into all elements that are under SLAs.

In support of the NCR's consideration of such an option, Respondent shall indicate the compliance level of its experience in providing access to third-party NOC/SOC overarching support, as related to the requirements identified in the following table:

**Table 1: Third-Party NOC/SOC Support**

Requirement	Complies	Complies Partially	Complies with Future Capability	Does Not Comply
4.9.13.1 Change management processes				
4.9.13.2 Coordinating and managing trouble tickets to resolution from Contractor and multiple suppliers				
4.9.13.3 Trouble ticket report management (reports may be daily, weekly, monthly, quarterly, or yearly)				
4.9.13.4 Notification processes for Contractor and suppliers, and any other entities or people designated by the NCR				

Requirement	Complies	Complies Partially	Complies with Future Capability	Does Not Comply
4.9.13.5 System alarm access in the form of SNMP or syslog data				
4.9.13.6 Experience and processes for interworking of multiple public safety voice and data system suppliers				

#### 4.9.14. Operational Scenarios

The NCR recognizes that no system or staff is perfect, however, safeguards may be established to minimize the impact of human or system error. Respondent shall describe its risk mitigation and issue resolution strategies for the following hypothetical scenarios:

1. At 0300 hours, a series of session border controller alarms previously unseen by the NOC staff on duty begin to increase in volume and frequency. At 0330, multiple critical alarms are received. At 0345, a few PSAPs start reporting garbled audio while others report an inability to obtain location information. At 0600, some NCR PSAPs are reporting that have not received a call in the last 15 minutes.

Response to hypothetical scenario:

2. All originating service providers in the NCR are directly connected via SS7 to the Respondent's two LNGs that are dedicated to the NCR. Each LNG consistently processes about 10,000 calls per day, but each is capable of processing in excess of 100,000 calls per day. One of the LNGs experiences a catastrophic failure and is unable to process any calls. In a review of the prior day's logs, it is found that the surviving LNG is only processing 14,000 calls.

Response to hypothetical scenario:

3. As part of normal data maintenance procedures, an NCR jurisdiction has uploaded six minor recent changes to its road centerline data. The Respondent's SI's QA/QC process provides a discrepancy report detailing 15,000 errors resulting from the updated file. The NCR GIS professional is confused and concerned that they've impacted live call routing.

Response to hypothetical scenario:

#### 4.10. NG9-1-1 CORE SERVICES (NGCS) ELEMENTS

Respondent shall provide a network or solution diagram that clearly depicts the Respondent's proposed transitional and end state for the ESInet and the NGCS, taking into account the jurisdictions listed in Attachment A. The diagram should depict the Option A scenario initially and then a second diagram should layer in Option B PSAPs. The following functional elements and services shall be included:

- Legacy Network Gateway (LNG)
- Legacy PSAP Gateway (LPG)
- Border Control Function (BCF)
- Emergency Services Routing Proxy (ESRP)
- Policy Routing Function (PRF)
- Emergency Call Routing Function (ECRF)
- Location Validation Function (LVF)
- Spatial Interface (SI)
- Location Database (LDB)
- Discrepancy Reporting
- Logging and Recording
- Time Server

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

##### 4.10.1. Legacy Network Gateway (LNG)

1. The LNG is a signaling and media interconnection point between callers in legacy call-originating networks (E9-1-1) and the NENA NG9-1-1 i3 architecture. The LNG shall log all calls it receives and processes and shall permit the uploading of daily log files to a network monitoring and management system for analysis. The LNG shall allow for ad hoc uploads of log files for troubleshooting and incident response. All call activity on both the legacy side (Time-Division Multiplexing, or TDM) and the IP side of the LNG shall be logged. The LNG shall have intrusion detection system (IDS)/intrusion prevention system (IPS) functionality to detect and mitigate distributed denial of service (DDoS) attacks from both the TDM side and the IP side.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The LNG shall provide the capability to obtain location information in order to define, create, populate and send the correct PIDF-LO parameter to the correct ESRP or terminating PSAP.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. The LNG shall obtain location information and create the correct Presence Information Data Format Location Object (PIDF-LO) message to pass on to the ESRP, as described within NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. The LNG shall convert all incoming 9-1-1 calls to Session Initiation Protocol (SIP) calls in accordance with the SIP requirements of NENA 08-003. Any Respondent variations and/or non-compliance with the SIP requirements of NENA 08-003 must be identified and noted.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. The LNG external interfaces shall comply with respective NENA requirements.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

6. The LNG shall support obtaining the callback number associated with any pseudo ANI data that does not include the callback number. This may require the Contractor to obtain the callback number from the wireless or Voice over Internet Protocol (VoIP) provider, and may include additional recurring and non-recurring costs that are independent of this RFP. The Contractor shall be responsible for all recurring and non-recurring costs associated with this requirement.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

7. The LNG must facilitate logging of all significant events and 9-1-1 calls received and processed. Each call log shall contain all relevant parameters defined in Section 5.11.3 of NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

8. All LNG logs files shall be capable of being extracted in near real-time, and shall be in a format suitable for importing into a spreadsheet or word processing program.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:



9. The LNG solution must be deployed with the resiliency and redundancy to provide a minimum of 99.999 percent availability.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

10. The LNG shall support star codes as defined in NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

11. Respondent shall describe how its LNG solution provides for Legacy Selective Router Gateway (LSRG) functionality.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

12. Respondent shall provide the proposed locations for hosting the primary LNGs for serving the NCR, including the data center tier level for the host sites.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.10.2. Legacy PSAP Gateway (LPG)**

1. The LPG is a signaling and media interconnection point between legacy PSAP customer premises equipment (CPE) and the NGCS. The LPG allows for the transfer of calls from the ESInet to a PSAP that may not have upgraded its CPE to an i3-capable call-handling

system. The LPG also allows the legacy PSAP to transfer or alternately route legacy TDM calls to another PSAP on the ESInet.

The LPG shall log all calls it receives and processes, and shall permit the uploading of daily log files to a network monitoring and management system for analysis. The LPG shall allow for ad hoc uploads of log files for troubleshooting and incident response in real-time or near real-time. All call activity on both the legacy (TDM) side and the IP side of the LPG shall be logged. The LPG shall have IDS/IPS functionality to detect and mitigate DDoS attacks from the IP side.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The LPG solution must be deployed with the resiliency and redundancy to provide a minimum of 99.999 percent availability.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. The LPG shall support a SIP interface toward the ESInet, as defined within NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. The LPG shall support both CAMA and ALI interfaces toward the PSAP CPE that are compliant with the requirements of NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. The LPG shall convert all incoming 9-1-1 calls to SIP calls in accordance with the requirements of NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

6. The LPG shall support star codes as defined in NENA 08-003, with the exception that the star codes may be up to three digits in length.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

7. The LPG must facilitate logging of all significant events and 9-1-1 calls received and processed. Each call log shall contain all relevant parameters given in Section 5.11.3 of NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.10.3. Border Control Function (BCF)**

1. The BCF shall provide logical network security functions between external networks and the ESInet, and between the ESInet and NCR agency networks. The BCF is responsible for numerous functions, including the following:
- Border firewall
  - VPN
  - IDS/IPS
  - Session Border Control (SBC)
  - Opening and closing of pinholes
  - Limiting access to critical components through the use of VLANs

- Call admission control
- Transcoding
- Signaling protocol normalization and interworking
- Network Address Translation (NAT)
- Codec negotiation
- Support for QoS and priority markings
- Media proxy

The Respondent shall provide details, including drawings depicting how its proposed BCF meets or exceeds all functions listed above and the requirements described in NENA 08-003, as well as additional firewall requirements described in NENA 04-503 and NENA 75-001, or the next subsequent version of the NENA documents listed that are publically available at the proposal release date.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The BCF solution shall be deployed in a manner to achieve 99.999 percent availability.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. Management of the BCF shall include auditing of system log files for anomalies, and processes for responding to and managing security incidents.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. The BCF must be capable of: detecting when silence suppression is present in the 9-1-1 call; continuing to use silent suppression if detected; and not enabling silence suppression if it is not detected in the call.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

5. The BCF shall mediate all incoming 9-1-1 calls from VoIP providers to SIP calls in accordance with NENA 08-003. Any specific variations or non-compliance with this requirement must be identified and documented.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

6. The BCF must provide the functionality to maintain logs of all 9-1-1 sessions and all additional BCF logging and recording requirements, as specified in NENA 08-003.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

7. The Contractor's BCF solution shall support transcoding of Baudot tones to real-time text, as described in IETF RFC 4103.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

8. The Respondent shall provide details on how its proposed SBC will recognize that a NAT or Network Address and Port Translation (NAPT) has been performed on Open Systems Interconnection (OSI) Layer 3, but not above, and correct the signaling message for SIP.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

9. The Respondent shall provide details on how its proposed SBC shall enable interworking between networks utilizing IPv4 and IPv6 through the use of dual stacks, selectable for each SBC interface, based on NENA 08-003. All valid IPv4 addresses and parameters shall be translated to/from the equivalent IPv6 values.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

10. The Respondent shall provide details on how its proposed SBC shall support SIP over the following protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Transport Layer Security over TCP (TLS-over-TCP), and Stream Control Transmission Protocol (SCTP). Protocols supported must be selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

11. The Respondent shall provide details on how its proposed SBC shall be capable of populating the Layer 3 headers, based on call/session type (e.g., 9-1-1 calls) in order to facilitate priority routing of the packets.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

12. The Respondent shall provide details on how its proposed SBC supports encryption for calls that are not protected entering the ESInet, based on NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

13. Respondent shall describe the functionality of the proposed BCF solution in sufficient detail to address the requirements outlined, with particular attention to the user interface and features, and the security aspects.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

14. The Respondent shall provide details, including drawings, depicting the different BCF elements that its proposed solution comprises. As part of the details, the Respondent shall provide all of the expected elements and/or interfaces to be provided by the NCR PSAPs to the Contractor.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.10.4. Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)**

1. The ESRP routes a call to the next hop. It also evaluates the originating policy rules set for the queue the call arrives on, extracts the location of the caller from the SIP signaling,

queries the ECRF for the nominal next hop route, evaluates the route based on policy rules and queue states of the downstream entity queues, and then forwards the call to the resulting next hop.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The PRF is a required function of the ESRP. The ECRF interacts with the PRF to determine the next hop of a call or event. Before the ESRP sends the call to the next hop, it first queries the PRF to check the status of the next hop to determine if a unique routing rule, or policy, is in place that would direct the call to another location. The destination of the next hop is typically a queue. The PRF monitors the downstream queues of ESRPs for active understanding of the entity's queue status.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. The PRF shall allow defining policy rules for distributing a wide range of calls in an efficient manner. Respondent shall describe their solution's Policy Store and the PSAP's ability to affect change to the PRF. Please describe the user interface, the authentication process, and the types of policy rules available at the time of proposal submission, as well as those on the product roadmap. Roadmap items should include an estimated time of feature availability.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:



4. A next-hop queue may be a uniform resource identifier (URI) that routes the call to an interactive multimedia response system (as described in IETF RFC 4240) that plays an announcement (in the media negotiated by the caller) and potentially accepts responses via Dual-Tone Multi-Frequency DTMF signaling, or other interaction protocols.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

5. The ESRP/PRF solution must be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

6. The Respondent shall provide an explanation of how its proposed ESRPs use the “options” transactions for maintaining “keep alive” between ESRPs, LNGs, LPGs and session recording services.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

7. The upstream interface on the proposed non-originating ESRPs shall implement Transmission Control Protocol/Transmission Layer Security (TCP/TLS), but must be capable of fallback to UDP, as described in NENA-08-003. SCTP support is optional. The ESRP shall maintain persistent TCP and TLS connections to the downstream ESRPs or user agents (UA) that it serves.

The Respondent shall provide detailed documentation describing how the non-originating ESRP interface supports TCP/TLS with fallback to UDP.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

8. The Respondent shall provide a description of how its ESRPs meet or exceed all functional requirements as defined in NENA 08-003, which are listed in the following table.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

**Table 2: ESRP Functional Requirements**

Requirement	08-003 Section	Complies	Complies Partially	Complies with Future Capability	Does Not Comply
4.10.4.8.1 Overview	5.2.1.1				
4.10.4.8.2 Call Queueing	5.2.1.2				
4.10.4.8.3 Queue State Event Package	5.2.1.3				
4.10.4.8.4 De-queue Registration Event Package	5.2.1.4				
4.10.4.8.5 Policy Routing Function	5.2.1.5				
4.10.4.8.6 ESRP Notify Event Package	5.2.1.6				
4.10.4.8.7 INVITE Transaction Processing	5.2.1.7				
4.10.4.8.8 BYE Transaction Processing	5.2.1.8				
4.10.4.8.9 CANCEL Transaction Processing	5.2.1.9				
4.10.4.8.10 OPTIONS Transaction Processing	5.2.1.10				
4.10.4.8.11 Upstream Call Interface	5.2.2.1				

Requirement	08-003 Section	Complies	Complies Partially	Complies with Future Capability	Does Not Comply
4.10.4.8.12 Downstream Call Interface	5.2.2.2				
4.10.4.8.13 ECRF Interface	5.2.2.3				
4.10.4.8.14 Location Information Server (LIS) Dereference Interface	5.2.2.4				
4.10.4.8.15 Additional Data Interfaces	5.2.2.5				
4.10.4.8.16 ESRP, PSAP, Call-Taker State Notification and Subscriptions	5.2.2.6				
4.10.4.8.17 Time Interface	5.2.2.7				
4.10.4.8.18 Logging Interface	5.2.2.8				
4.10.4.8.19 Data Structures	5.2.3				
4.10.4.8.20 Policy Elements	5.2.4				
4.10.4.8.21 Provisioning	5.2.5				

#### 4.10.5. Emergency Call Routing Function (ECRF)

1. The ECRF shall be designed according to NENA 08-003 and be implemented using diverse, reliable and secure IP connections.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

2. Contractor shall supply an ECRF function that meets a minimum of 99.999 percent availability.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

3. Contractor providing an ECRF must ensure that it is accessible from outside the ESInet and that the ECRF permits querying by an IP client/endpoint, an LNG, an ESRP in a next-generation emergency services network, or by some combination of these functions.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

4. An ECRF accessible inside an ESInet must permit querying from any entity inside the ESInet. ECRFs provided by other entities may have their own policies regarding who may query them.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

5. An origination network may use an ECRF, or a similar function within its own network, to determine an appropriate route—equivalent to what would be determined by the authoritative ECRF—to the correct ESInet for the emergency call. Respondent shall describe the functionality of such an ECRF equivalent and document where this functional element resides within its proposed solution.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

6. The ECRF shall support a routing query interface that can be used by an endpoint, ESRP, or PSAP to request location-based routing information from the ECRF. Additionally, it must support both iterative and recursive queries to external ECRF sources.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

7. The ECRF must interface with the LoST protocol (as described in IETF RFC 5222) and support LoST queries via the ESRP, PSAP CPE, or any other permitted IP host.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

8. The proposed ECRF must allow for rate-limiting queries from sources other than the proposed ESRP(s), and provide logging of all connections, connection attempts, and LoST transactions.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

9. The ECRF must support:
- Logging of all connections, connection attempts, data updates, ECRF query results and LoST transactions
  - Location error correction
  - Updates from the SI in near real-time with no degradation of LoST services
  - Routing of calls based on geographic coordinates, geodetic shapes and civic addresses
  - Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire and emergency medical services (EMS)
  - Permitting of LoST queries for find service request association with each layer
  - Compliance with NENA 02-010 and NENA 02-014
  - Dynamic updates to GIS without disruption of the ECRF
  - Validation of GIS updates before they are provisioned into the ECRF

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

10. Respondent shall define its method for: provisioning the ECRF; updating the ECRF (including the frequency of updates); validating data provisioning; performing error logging; performing gap and overlap analysis; and supporting LoST queries from ESRPs, the PSAP CPE, and other authorized hosts within the ESInet. The Respondent shall provide a clear description of the functionality of the ECRF, list features and capabilities, describe its error handling, default mechanisms and logging, and provide an overview of deployment recommendations to achieve 99.999 percent reliability.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

11. The NCR acknowledges that its ESInet will be part of an overall hierarchical plan that includes interconnectivity to other regions and state-level ECRFs. The Respondent shall provide details regarding its vision for how this interconnection will include replicas of ECRF/LVF at different levels of the hierarchy, as well as access/origination networks.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

12. Respondent shall provide explanations of any tradeoffs between aggregations of data at higher-level ECRFs versus the use of Forest Guides to refer requests between ECRFs that possess different levels of data. As part of that explanation, the Respondent shall provide details on how the appropriate ECR/LVF data should be provisioned for use in overload and backup-routing scenarios, and any dependencies that might impact provisioning.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

#### **4.10.6. Location Validation Function (LVF)**

1. An LVF is a LoST protocol server where civic location information for every call originating

endpoint is validated against the SI-provisioned GIS data. The SI is responsible for provisioning and updating the information used for location validation in the LVF, which shall contain a standardized interface to the SI.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The LVF must be available to validate civic locations at the time a wireline device is ordered (Service Order Interface [SOI] validation), when a nomadic device is connected to the network, and when a PSAP or other authorized entity makes a civic location validation request. The LVF shall periodically reevaluate the civic location information contained in the Location Database.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. The LVF shall support all functionality as defined in NENA 08-003, shall be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability, and shall be provisioned with the same data as the ECRF.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. The Respondent should outline options for a public-facing LVF provisioned for use by service providers outside the ESInet.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. Respondent shall describe the functionality of the proposed LVF solution in sufficient detail to address the requirements outlined, with particular attention to the arrangement of the proposed components, user interface and features, and security aspects.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

#### 4.10.7. Spatial Interface (SI)

1. The SI is responsible for provisioning and updating authoritative GIS data to the ECRF, the LVF, the map viewer, the PSAP tactical map display, computer-aided dispatch (CAD) systems, and similar applications that consume GIS data. GIS data provisioned by the SI must undergo data quality and data integrity checks to ensure that the data complies with all applicable requirements of NENA 02-010, NENA 02-014, and Attachment B of NENA 08-003.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

2. The SI shall convert the GIS data meeting these requirements into the LoST protocol used by the ECRF and LVF, in real-time or near real-time, using a Web feature service. The SI shall be able to provision and perform incremental updates, in near real-time, to the ECRF, LVF, the map viewer service, the PSAP tactical map display and similar applications that consume GIS data.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:



3. Respondent shall describe the functionality of the proposed SI solution in sufficient detail to describe the validation of GIS data and data updates prior to their provisioning into the ECRF and LVF, along with the means of real-time or near real-time provisioning of incremental updates to the GIS data provisioned to the ECRF and LVF.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

4. Respondent shall describe how it will use the region's GIS data model (Attachment B) and align with the region's data maintenance processes with minimal impact to existing data maintenance operations. Respondent shall define its processes and methods to receive and incorporate the SI datasets that have been prepared by the region as previously described and as defined in Attachment B. Respondent shall describe its proposed workflow for receiving GIS updates from jurisdictions, to allow for a smooth transition from the existing processes that have been implemented during the preparation of the region's NG9-1-1 data by the jurisdictions. Respondent also must describe all security and monitoring aspects, and any additional features supported by the proposed SI.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

#### **4.10.8. Location Database (LDB)**

1. A Location Database (LDB) serves as both a legacy ALI database and as an LIS in an i3 NG9-1-1 environment. The LDB retains all of the current information, functionality, and interfaces of today's ALI, but also can utilize the new protocols required in an NG9-1-1 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center (MPC) or gateway mobile location center (GMLC), and the protocols required for i3 location information retrieval and conveyance, such as HTTP-Enabled Location Delivery (HELD) or other proprietary protocols.

The LDB must meet the following requirements:

- Shall support all relevant sections of NENA 02-010, 02-011, 02-015, 04-005, 08-501 and 08-502 related to ALI DBMS
- Shall be capable of assuming the role of a location DBMS as defined in the NENA NG9-1-1 Transition Plan Considerations (NENA-INF-008.2-2013)
- Shall support NENA standards (J-036, E2, E2+, NCAS, CAS)
- Shall be able to provide LIS functionality and interfaces as defined in NENA 08-003
- Shall be able to seamlessly interact with a NENA i3 ECRF, as described in NENA 08-003
- Shall be able to dereference a location by reference, as defined in NENA 08-003
- Shall be able to dereference requests for additional information, as defined in NENA 08-003
- Shall be able to interface simultaneously with multiple wireless callers
- Shall be able to interface simultaneously with multiple remote ALI databases
- Shall automatically detect, import and validate customer records (SOI records)
- Shall have the ability to be used simultaneously by both NG9-1-1-capable and E9-1-1-capable PSAPs
- Shall allow different PSAPs to use different ALI formats based on individual needs
- Shall utilize LVFs to validate civic addresses
- Shall support location data formatting as defined in the NENA Civic Location Data Exchange Format (CLDXF)
- Shall periodically reevaluate the location information using LVF functions within the system
- Shall be able to communicate with NG9-1-1 functional elements using the HELD protocol
- Shall be able to provide a PIDF-LO based on both the wireless and VoIP E2 response
- Shall be able to dereference additional data request
- Shall consistently respond to all requests within 400 ms

Respondent shall describe the functionality of the proposed LDB, including additional features and capabilities, error handling, logging and deployment recommendations in sufficient detail to address the requirements outlined, with particular attention to the arrangement of the proposed components, user interface and features, and security aspects.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

2. The LDB shall support the integration of private ALI databases. The Metropolitan Washington Airports Authority (MWAA) provides 9-1-1 call-taking and dispatch services for Dulles International Airport, Reagan National Airport, and the Dulles Toll Road. The MWAA PSAP handles wireline calls that originate in its jurisdictions directly, and receives transfers from neighboring NCR PSAPs for wireless and VoIP calls. The PSAP's call-handling equipment initially bids two onsite private ALI databases and if no record is found, it will bid the Verizon ALI nodes. As part of this migration, Contractor shall be responsible for migrating approximately 7,500 records from the MWAA private ALI databases to the LDB.

Respondent shall provide details on the database migration process and the user interface for MWAA staff to manage these private ALI records.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.10.9. Discrepancy Reporting**

The Respondent shall provide details regarding its proposed solution's report functions for notifying agencies any time a discrepancy is detected with the BCF, ESRP, PRF, ECRF, LVF, and SI. As part of the detail, the Respondent shall explain how a report will be sent for the purpose of reporting the discrepancy to multiple responding agencies, as determined by the NCR. Discrepancy reporting is outlined in Section 4.9 of NENA 08-003. Respondent shall describe the functionality of the proposed discrepancy reporting function in sufficient detail to address the requirements outlined, with particular attention to the user interface and features, and the security aspects.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.10.10. Event Logging and Management Information System (MIS)**

1. Extensive logging of NG9-1-1-related events, transactions, media and operations is required. Logging includes all elements in the call flow including logging of events within ESInets, the NGCS, the PSAP and related operations, and is a standardized function used throughout ESInets, NG9-1-1 functional elements and PSAPs. Logged events include

ingress and egress to an ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall describe how its event logging solution may integrate with each PSAP's call-handling equipment to provide a complete, end-to-end view of a call and/or describe how a PSAP can gain access to information in the event logging solution. Respondent shall describe requirements of the PSAP's call-handling equipment, software license agreements, software licensing costs, and interfaces required to support integration with the Respondent's event-logging solution.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. Respondent shall describe how a PSAP can gain access to the event-logging solution to review recordings and run statistical and other MIS reports. Respondent shall describe retention periods associated with all logging records.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. Because logs may be subpoenaed and used as a source of information in legal proceedings, the logging systems shall be designed, proposed, and operated with legal defensibility of logged information taken into careful account. All log entries shall be accurately time stamped.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. The Contractor's proposed logging solution must meet the requirements set forth in NENA 08-003.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

6. Contractor is responsible for any third-party certification fees.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

7. Respondent shall describe the reports, MIS tools, and performance metrics made available to each PSAP, the user interface for retrieving or receiving reports, and the ability to customize reports based on individual PSAP needs. The NCR desires reports and metrics that include but are not limited to:

- Timing
  - Call delivery time
  - Call processing time between elements
- Volumes
  - Call volumes by call type
  - Alternate-routed calls
  - Text-to-9-1-1
  - All NGCS element usage volumes
- Bandwidth/trunk utilization
  - Calls per trunk
  - Trunk utilization
  - Circuit utilization
- Call Flows and Agent Activity

- Call transfers
- Call conferences
- End-to-end call-flow analysis

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.10.11. Network Time Protocol (NTP) & Time Source**

1. Contractor shall provide redundant, resilient network-attached time sources (“master clocks”) capable of supplying standard time to all systems, network devices, and functional elements that comprise the ESInet and the NGCS.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The master clock time source(s) shall be accessible to the PSAPs for synchronizing their call-handling systems and other related systems. All systems, network devices, and functional elements shall support the use of the Network Time Protocol (NTP) for maintaining system clock accuracy.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.10.12. NG9-1-1 Applications and Alarm Integration**

1. NG9-1-1 provides for the capability to have alarm companies integrate directly with the ESInet and use the NGCS for routing of the alarm and its associated data. The NCR is interested in implementing such capabilities. As an optional service and priced separately, Respondent may describe its experience in integrating alarm and sensor data with its NGCS solution.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. As an optional service and priced separately, Respondent may describe other NG9-1-1 applications, Additional Data integrations, and personal safety applications that may be integrated with its NGCS solution.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.10.13. Message Session Relay Protocol (MSRP) Text Integration**

Multiple NCR PSAPs have deployed short messaging service (SMS) to 9-1-1 service, with several others planning to do so in the next year. The text control centers (TCC) of both West and Comtech TCS are serving the region through a variety of direct MPLS network connectivity and Internet-based access. Respondent shall describe its ability to integrate existing Web-based and MSRP-integrated SMS to 9-1-1 and future RTT into its ESInet. Respondent shall explain whether its solution supports location-by-reference and/or location-by-value. This requirement is for integration of text messaging with MSRP and not a requirement for procuring text services. Respondents shall provide costs for MSRP integration with the NGCS in the Optional Costs Pricing table.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.11. SERVICE LEVEL AGREEMENTS (SLA)**

##### **4.11.1. System Capacities and Performance**

Respondent shall provide capacity levels of each element of the ESInet and the NGCS. This may be in terms of busy-hour calls, network bandwidth, or any other applicable measure. The proposed solution must be capable of handling current call volume plus 25 percent growth over the term of

the contract. Respondent shall provide the incremental cost to handle 125% of current call volume in the Optional Pricing Table. Respondent shall specify lead times required to increase capacities on each element of the ESInet and the NGCS.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### 4.11.2. System Performance

1. *Network Latency*—Respondent shall specify the guaranteed maximum latency across its backbone network under a full-load condition, and include how that information will be gathered, calculated and provided to the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. *Point of Presence (POP) to POP*—Respondent shall specify the guaranteed maximum latency from interconnection facility (aka, point of presence, or POP) to interconnection facility, and include how that information will be gathered, calculated and provided to the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. *POP to Endpoints*—Respondent shall specify the guaranteed maximum latency from interconnection facilities to the network interface device located at the entrance to the customer's premises, and include how that information will be gathered, calculated and provided to the NCR.



- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. *Packet Loss*—Respondent shall specify the guaranteed maximum end-to-end packet loss across its network. This specification also shall include any loss characteristics associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. *Network Traffic Convergence*—Respondent shall specify convergence protocols and the estimated or guaranteed network convergence time (<54 milliseconds [ms]) of IP traffic at any point within the proposed solution, including how convergence information will be gathered, calculated and provided to the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

6. *Mean Time to Repair*—Respondent shall specify the mean time to repair (MTTR) characteristics of its proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Respondent shall include how MTTR information will be gathered, calculated and provided to the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

7. *Mean Time Between Failures*—Respondent shall specify the mean time between failures (MTBF) characteristics of its proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Respondent shall include how MTBF information will be gathered, calculated and provided to the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

8. *System Availability*—Respondent shall specify the service level offered as a percentage of time when the service is available, and the maximum period of total outage before remedies are activated. Availability is defined as  $MTBF/(MTBF+MTTR)$ . Respondent shall include how system availability information will be gathered, calculated and provided to the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

9. *End-of-Support Equipment*—Contractor shall proactively replace any hardware that has reached end of support (EOS) no later than 90 days prior to the manufacturer's EOS date.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

10. *Remedies*—Respondent shall define the financial and operational remedies to the NCR and its respective specified agencies for each event in which the above system performance service levels are not maintained.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.11.3. SLAs for Incident Management**

It is expected that the Contractor will have processes and procedures for supporting a NOC/SOC that can rapidly triage calls. Respondent shall describe the attributes of its incident severity levels, including response and resolution times for each severity level, and how response and resolution times are measured.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.11.4. Outage Notification and Reason for Outage (RFO) Report**

1. Contractor shall comply with all applicable FCC rules throughout the term of the services contract.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Contractor shall notify the NCR jurisdictions and/or its designee within 30 minutes of discovering an outage that may impact 9-1-1 services. At the time of initial notification, the Contractor shall convey all available information that may be useful in mitigating the effects of the outage, as well as a name, telephone number, ticket or reference number, and email address at which the service provider can be reached for follow-up. The Contractor is responsible for coordinating data gathering, troubleshooting and reporting on behalf of its suppliers.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. Contractor shall communicate any additional material information to the NCR or its designee no later than two hours after the initial contact, and at intervals no greater than two hours thereafter until normal 9-1-1 service is restored. This information shall include the nature of the outage, its best-known cause, the geographic scope of the outage, the estimated time for repairs, and any other information that may be useful to the management of the affected facility.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. Following the restoration of normal 9-1-1 service, Contractor shall provide a Reason for Outage (RFO) Report/Root Cause Analysis to the NCR jurisdictions and/or its designee, no later than 30 days after discovering the outage. Respondent shall describe its compliance with the notification and reporting requirements stated above. Respondent shall describe the NOC/SOC tools and techniques at its disposal to ensure that its various suppliers perform troubleshooting and post-event analysis, and provide associated reports.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. Outage notifications are a critical element to understanding overall system health. Having awareness of issues that exist in a neighboring NCR PSAP provides valuable insight to potential issues that may begin impacting another PSAP's operations. For example, if PSAP A's trunk capacity is impaired and PSAP B is PSAP A's first defined alternate route, then having insight to the impaired capacity issue will assist PSAP B in preparing staff for managing the potential influx of calls from PSAP A.

As such, the NCR is interested in an outage notification service that allows for each PSAP to elect the outage notification types and PSAPs for which it will receive outage

notifications, outage updates and RFO reports. A Web portal for authorized users to select/deselect outage notifications is preferable.

Respondent shall provide a detailed description of how it may be able to support such an outage notification service.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.11.5. SLA Reporting**

Respondent shall provide a detailed description of how it measures and reports incidents, including immediate notifications and regularly scheduled reports. The mechanism shall deliver SLA results to the NCR and its designees on a monthly basis. The report shall include all performance items identified in the Contractor's proposal and documented in contract negotiations.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### **4.11.6. SLA Violations**

An SLA violation shall have occurred whenever:

- The Contractor fails to meet any single performance level
- The average of any single performance item over the preceding two-month period fails to meet the service level. This is an "early warning" of an unacceptable trend.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### 4.11.7. Incident Severity Level 1 and 2 Violation Damages

Contractor shall provide financial remedies to the NCR and its respective specified agencies for each event in which service levels are not maintained. The NCR expects that all of the Contractor's network devices and services will perform at a level equal to 99.999 percent uptime measured on a rolling, 12-month calendar. Failure to meet SLAs shall be measured per service-affecting outage. Penalties shall be assessed for failure to meet SLAs. The Respondent shall include how uptime information will be gathered, analyzed and provided to NCR.

For Severity Level 1 and 2 incidents, a 10-percent penalty shall be assessed against the monthly recurring fee (MRF) whenever the initial period of resolution is exceeded. If the resolution period length of time doubles, then the penalty shall increase to 20 percent of the MRF. If the resolution period length of time quadruples the initial period, then 50 percent of the MRF shall be assessed. The amount related to the damages is to be credited to the invoice of each affected NCR jurisdiction the month immediately following the violation.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

#### 4.12. PSAP INTERFACES AND BACKROOM EQUIPMENT REQUIREMENTS

1. The PSAP call interface is a SIP call interface as described in NENA 08-003. The geolocation header, call information headers and other headers shall be the same as described in NENA 08-003. The call will be routed, using normal RFC 3261 procedures, to the URI obtained from the ESRP's PRF. See NENA 08-003, Section 5.6 for other information on the PSAP interface.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Contractor's solution shall support PSAP interfaces specified in NENA 08-003, Section 4.1, including the following:
  - SIP call interface
  - SIP subscribe and notify
  - Support for Web services

- Support for HELD and LoST queries and responses
- Support for placing abandoned call return
- Support of SIP call transfer, call bridging, and call conferencing
- Support for all baseline media and multimedia as described in NENA 08-003, Section 4.1
- Support for ad hoc location validation
- Support for queries to and responses from additional data repositories
- Support for NTP time services interface, accurate to 1 millisecond
- Support for logging of all calls, queues, upstream element states, and incoming calls and their associated media
- Support for Transport Layer Security
- Support for the NENA/ APCO Emergency Incident Data Document (EIDD)
- Support for Short Message Service (SMS), instant messaging and star code equivalent transfers
- Support for test calls

Respondent shall describe the functionality of the PSAP interfaces in sufficient detail to address the requirements outlined, with particular attention to the user interface, additional features, and security aspects.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. Based on the CPE listed in Attachment A, Respondent shall provide a list of CPE platforms for which it has successfully implemented the interfaces listed above in a live production environment, noting any interfaces that have not yet been tested with each CPE vendor/model. Where interfaces with CPE vendors/models have yet to be deployed and/or tested, please describe the integration testing process that the Respondent will perform prior to acceptance testing of the solution. Please note the expected physical interface handoff at the PSAP CPE demarcation point.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. The NCR anticipates that equipment such as routers, firewalls, network management consoles, and other equipment will be required to be housed at the PSAPs. Respondent shall describe each piece of equipment that is required at each location type by filling in the following tables. Respondent shall assume that they will provide the appropriate equipment cabinet to house the required equipment at each PSAP. Respondent shall describe the backroom footprint required for the solution equipment for the respective PSAP.

- ☐ Complies  
☐ Complies Partially  
☐ Complies with Future Capability  
☐ Does Not Comply

Details to support the answer:

**Table 3: PSAP with CPE (including CPE host sites)**

Equipment Type	Vendor/Model	Equipment Type	Function	Rack Units	Heat Load (BTU/hr.)	Relative Humidity	Power Requirements (VAC or VDC, amperes load)

PSAP with CPE Footprint Description:

**Table 4: Remote PSAPs (if applicable)**

Equipment Type	Vendor/Model	Equipment Type	Function	Rack Units	Heat Load (BTU/hr.)	Relative Humidity	Power Requirements (VAC or VDC, amperes load)

Remote PSAP Footprint Description (if applicable):



## 5. MIGRATION PLAN OPTIONS

1. Respondent shall describe its proposed migration plan to the NG9-1-1 system from the existing E9-1-1 system, highlighting any potential disruption to existing operations at each PSAP, as well as any costs the Respondent is relying on the PSAP or NGCS project to cover. Also, any specific dependencies the Respondent has for a successful implementation that are seen as PSAP responsibilities should be explained clearly. The NCR seeks a migration plan that provides for the most cost-effective migration while ensuring the integrity of the region's mission-critical 9-1-1 services. Respondent shall describe how its solution minimizes reliance on legacy selective routers and ALI database services. This detail shall include ingress network design, ESInet design, data center build plans, a clear project schedule of activities (including Gantt charts), example test plans, process audits, risk mitigation plans, and staffing plans.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The Respondent shall provide a Master Project Plan (MPP) that depicts the major sequencing of project activities and the timeline for each activity. Within 60 days of successful contract award, the Contractor shall develop an implementation plan for each jurisdiction's individual PSAPs, identifying any unique characteristics and tasks that are required for integration with each PSAP's call-handling system and the Contractor's NGCS solution, using aforementioned i3 protocols such as SIP, PIDF-LO, LoST, HELD, and HTTP GET.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. Respondent's migration plan shall describe its proposed specific sequence of PSAP migrations, considerations that may influence such sequencing, and if any PSAP sequences are mandatory.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. Respondent shall provide examples of where this migration methodology has been successfully deployed in the past.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. Respondent shall describe any steps that the PSAPs should take to streamline the migration project, with descriptions of required resources and details regarding what is required versus optional.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

## **6. PROJECT MANAGEMENT AND ON-GOING CLIENT MANAGEMENT SERVICES**

1. Respondent shall describe its project management methodology and support structure. Please describe the daily, weekly, and monthly interactions during the migration.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall identify by name and provide resumes for the specific project team that will manage the migration.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. Respondent shall provide a description of each team member's role and their anticipated amount of time dedicated to the project. Respondent shall describe key team members' experience in managing and implementing projects of similar size and scope.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. Contractor shall not change key staff during the course of the project without mutual agreement with the NCR and/or the Fairfax County Purchasing Agent. The NCR desires for Respondents to bring key staff members to oral presentations, if invited.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

5. Respondent shall describe the post-deployment client management service, including client management reports, executive briefings and the fielding of ad hoc support requests.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

## 7. TRAINING

1. Contractor shall provide comprehensive training for the implementation process and ongoing maintenance of the NGCS and ESInet. Respondent shall describe its training program, including but not limited to the following topics: trouble reporting, help desk Web interface, PRF policy store interface, SI discrepancy reporting, LDB data management, and service monitoring tools.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall describe the types of attendees required to attend training, training curriculum, number of training attendees included in the proposed price, and the duration of the training program per attendee (expressed in hours per day and number of days), as well as the location of the training and whether such training is available online. Preference is given to training that can be conducted within the NCR. Examples of proposed training plans and training materials are desired.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

## 8. SERVICE, REPAIR AND ADVANCE REPLACEMENT

As this is a service-based offering, the NCR shall not be responsible for the replacement and maintenance of hardware and software required to provide the ESInet and the NGCS. Contractor must resolve all faults or malfunctions at no additional cost to the NCR.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

## **9. SOFTWARE RELEASE POLICY**

### **9.1. SCHEDULED RELEASES**

1. Respondent shall describe the frequency of scheduled software releases, the feature release testing process, and the decision-making processes involved in deciding what features and defect resolutions to include in a scheduled release.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. Respondent shall explain how it replicates the client environment for software release testing in order to provide assurances that future software releases will not negatively impact PSAP operations.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

### **9.2. MAINTENANCE RELEASES**

1. Respondent shall describe the frequency of defect resolution software releases, as well as the decision-making processes involved in selecting which software defects to fix.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

2. The Contractor shall provide the NCR with access to the Contractor's defect tracking system in order for the NCR to track the progress of defect resolutions.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

3. The Contractor shall provide a detailed description of the software defect tracking process and provide training to NCR staff prior to Final Acceptance Testing.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

4. Respondent shall describe how software defects are aged. For example, a minor problem (from the Respondent's perspective) can become a major or critical problem if not resolved in a timely manner. For example, a column of numbers in an MIS report may not total properly. While this certainly is not a service-affecting problem, it does make the PSAP administrator's job more difficult if these totals have to be maintained separately and totaled manually. Using this example, the Respondent shall describe in detail how/when this minor problem gets scheduled or automatically escalated, and the feedback mechanism in place for keeping the NCR PSAPs informed.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

## 10. DOCUMENTATION

The Contractor shall provide each of the NCR PSAPs with pertinent documentation for the ESInet and NGCS, and update the NCR PSAPs as configurations change over the term of the contract.

The required documentation shall include the following:

- Customized migration plan
- Escalation procedures
- Circuit identification
- Single points of failure

- Network path diversity drawings into each data center
- Network path diversity drawings into each PSAP
- PSAP backroom as-built drawings
- PSAP demarcation point drawings
- All user interface training and reference materials

The Contractor shall provide all documentation in agreed-upon soft copy format. Additionally, access to documentation on a Contractor-hosted Web-portal is desired.

- ☐ Complies
- ☐ Complies Partially
- ☐ Complies with Future Capability
- ☐ Does Not Comply

Details to support the answer:

### Attachment A: NCR PSAP Data for Proposed ESInet and NGCS

PSAP	PSAP Type*	Street Address	City	ST	ZIP	NPA-NXX	2014 Pop-ulation	# Dis-patched Calls	9-1-1 Call Transfer	Wire-line Trunks	Wire-less Trunks	# of Work-stations	SR	ALI	CPE
Alexandria Police Department	Pri		Alexandria	VA	22304	703-746	150,575	72,575		12	16	31	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	Airbus DS Sentinel 3.1
Alexandria PD Backup PSAP	Bckp			VA			n/a					11	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	
Alexandria Fire Communications	Sec		Alexandria	VA	22314	703-746	n/a			Assume 4 or less		Assume 4 or less			
Arlington County Emergency Communications Center	Pri		Arlington	VA	22201	703-228	229,164	115,991	28,415	16	16	30	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	Airbus DS VESTA Meridian 2.2 (SP-4)
Arlington County ECC Backup PSAP	Bckp		Arlington	VA	22201	703-228	n/a					13	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	Airbus DS VESTA 2.2 SP 4 1000E
Falls Church Police Communications (within Arlington jurisdiction)	Sec		Falls Church	VA	22046	703-248	n/a			Assume 4 or less		Assume 4 or less			Airbus VESTA 4.0
Fairfax County Public Safety Communications Center	Pri (Side A geodiversion)		Fairfax	VA	22030	571-350	1,137,538	670,000	37,799	14 (includes 4 VoIP)	14	57	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	Airbus VESTA 6.0
Fairfax County PSCC Alternate PSAP	Bckp (Side B geodiversion)		Annandale	VA	22003	703-280	n/a			14 (includes 4 VoIP)	14	21	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	Airbus VESTA 6.0
Fairfax City Police Communications	Sec		Fairfax	VA	22030	703-385	n/a								Remote off Fairfax County
Herndon Police Communications	Sec		Herndon	VA	20170	703-435	n/a	25,013		4		5	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	Remote off Fairfax County



PSAP	PSAP Type*	Street Address	City	ST	ZIP	NPA-NXX	2014 Population	# Dispatched Calls	9-1-1 Call Transfer	Wire-line Trunks	Wire-less Trunks	# of Work-stations	SR	ALI	CPE
Vienna Police Communications	Sec		Vienna	VA	22180	703-255	n/a			Assume 4 or less		Assume 4 or less			Remote off Fairfax County
Fauquier County 9-1-1 Dispatch Center	Pri		Warrenton	VA	20186	540-347	68,248	108,194	NA			7	Verizon Fairfax/Alexandria and Fredericksburg /Winchester	Verizon Richardson/Longmont	Airbus DS VESTA
Manassas City Police Communications	Sec		Manassas	VA	20110	703-257	42,081			Assume 4 or less		Assume 4 or less			
Manassas Park Police Communications	Sec		Manassas Park	VA	20111	703-361	15,174	21,974		4	0	3	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	Airbus DS VESTA 2.6
Metropolitan Washington Airport Authority	Pri		Sterling	VA	20166	703-417	120,548					20	Verizon Fairfax/Alexandria	Private ALI and Verizon Richardson/Longmont	Airbus Vesta
Prince William County Public Safety Communications	Pri		Lake Ridge	VA	22192	703-792	446,094	381,865	216	5	5	15	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	West VIPER A9C 4.0
Prince William County Public Safety Communications Backup PSAP	Bckp		Manassas	VA	20110	703-368	n/a			5	5	8	Verizon Fairfax/Alexandria	Verizon Richardson/Longmont	West VIPER A9C 4.0
Stafford County Sheriffs Communications	Pri		Stafford	VA	22554	540-659	139,992	170,799	17,192	8	10	25	Verizon Fairfax/Alexandria and Fredericksburg /Winchester	Verizon Richardson/Longmont	Emergency Call Works
Stafford County Sheriffs Communications Backup PSAP	Bckp			VA			n/a					5	Verizon Fairfax/Alexandria and Fredericksburg/ Winchester	Verizon Richardson/Longmont	Emergency Call Works

PSAP	PSAP Type*	Street Address	City	ST	ZIP	NPA-NXX	2014 Pop-ulation	# Dis-patched Calls	9-1-1 Call Transfer	Wire-line Trunks	Wire-less Trunks	# of Work-stations	SR	ALI	CPE
<b>PART B PSAPs</b>															
Calvert County PSAP	Pri		Prince Frederick	MD	20678	410-535	90,613	34,072				14	Verizon Hyattsville/ Rockville	Verizon Richardson/ Longmont	Airbus DS VESTA
Calvert County Backup PSAP	Bckp		Prince Frederick	MD	20678	410-535							Verizon Hyattsville/ Rockville	Verizon Richardson/ Longmont	Airbus DS VESTA
Charles County 9-1-1 Communications Center	Pri		La Plata	MD	20646	301-609	154,747	35,607		4	4	16	Verizon Hyattsville/ Rockville	Verizon Richardson/ Longmont	Airbus DS VESTA 2.2
Charles County 9-1-1 Communications Backup PSAP	Bckp		La Plata	MD	20646	301-934	n/a			4	2	4	Verizon Hyattsville/ Rockville	Verizon Richardson/ Longmont	Airbus DS VESTA 2.2
Frederick County Emergency Operations Center	Pri		Frederick	MD	21701	301-600	243,675	324,824	651	8	12	28	Verizon Pikesville/ Ellicott City	Verizon Richardson/ Longmont	Airbus VESTA 6.0
Frederick County Emergency Operations Center Backup PSAP	Bckp		Frederick	MD	21701		n/a			8	12	18	Verizon Pikesville/ Ellicott City	Verizon Richardson/ Longmont	
Frederick Police Department	Sec		Frederick	MD	21701	301-694	n/a			Assume 4 or less		Assume 4 or less			
Montgomery County Police Communications Center	Pri		Gaithersburg	MD	20878	301-869	1,030,447	354,468	135,714	18	20	41	Verizon Hyattsville/ Rockville Verizon Southwest/ Anacostia	Verizon Richardson/ Longmont	Intrado VIPER ICC/ Power911
Montgomery County Police Communications Center Backup PSAP	Bckp		Rockville	MD	20850	301-217	n/a			19	20	32	Verizon Hyattsville/ Rockville Verizon Southwest/ Anacostia	Verizon Richardson/ Longmont	Intrado VIPER ICC/ Power911
Takoma Park Police (within	Sec		Takoma Park	MD	20912	301-270	n/a			Assume 4 or less		Assume 4 or less			Remote off

PSAP	PSAP Type*	Street Address	City	ST	ZIP	NPA-NXX	2014 Pop-ulation	# Dis-patched Calls	9-1-1 Call Transfer	Wire-line Trunks	Wire-less Trunks	# of Work-stations	SR	ALI	CPE
Montgomery County jurisdiction)															Montgomery County
Prince Georges County Emergency Communications Center	Pri		Bowie	MD	20715	301-333	904,430	1,367,591	66,031	20	17	76	Verizon Hyattsville/Rockville	Verizon Richardson/Longmont	Airbus DS VESTA 6.0
Prince Georges County Emergency Communications Center Backup PSAP	Bckp		Landover	MD	20785	301-324	n/a			20	13	43	Verizon Hyattsville/Rockville	Verizon Richardson/Longmont	Airbus DS VESTA 6.0
St. Mary's County	Pri		Leonardtown	MD	20650	301-475	110,382	15,650				14	Verizon Hyattsville/Rockville	Verizon Richardson/Longmont	VESTA 2.2

\* PSAP TYPE LEGEND: Pri = Primary; Bckp = Backup; Sec = Secondary

Attachment B: NCR GIS Data Model

Table 5: Address Data Model

Name	Type	IsNullable	Length
OBJECTID	esriFieldTypeOID	FALSE	4
SHAPE	esriFieldTypeGeometry	TRUE	0
SITE_UNIQUE_ID	esriFieldTypeString	TRUE	100
SOURCE_OF_DATA	esriFieldTypeString	TRUE	75
EFFECTIVE_DATE	esriFieldTypeDate	TRUE	8
EXPIRATION_DATE	esriFieldTypeDate	TRUE	8
DATE_UPDATED	esriFieldTypeDate	TRUE	8
ADDRESS_NUMBER_PREFIX	esriFieldTypeString	TRUE	15
ADDRESS_NUMBER	esriFieldTypeSmallInteger	TRUE	2
ADDRESS_NUMBER_SUFFIX	esriFieldTypeString	TRUE	15
UNIT	esriFieldTypeString	TRUE	75
BUILDING	esriFieldTypeString	TRUE	75
FLOOR	esriFieldTypeString	TRUE	75
ROOM	esriFieldTypeString	TRUE	75
SEAT	esriFieldTypeString	TRUE	75
PLACE_TYPE	esriFieldTypeString	TRUE	150
COMPLETE_LANDMARK_NAME	esriFieldTypeString	TRUE	50
STREET_NAME_PRE_MODIFIER	esriFieldTypeString	TRUE	30
STREET_NAME_PRE_DIRECTIONAL	esriFieldTypeString	TRUE	12
STREET_NAME_PRE_TYPE	esriFieldTypeString	TRUE	30
STREET_NAME_PRE_TYPE_SEPARATOR	esriFieldTypeString	TRUE	30
STREET_NAME	esriFieldTypeString	TRUE	75
STREET_NAME_POST_TYPE	esriFieldTypeString	TRUE	30
STREET_NAME_POST_DIRECTIONAL	esriFieldTypeString	TRUE	12
STREET_NAME_POST_MODIFIER	esriFieldTypeString	TRUE	30
INCORPORATED_MUNICIPALITY	esriFieldTypeString	TRUE	100
UNINCORPORATED_COMMUNITY	esriFieldTypeString	TRUE	100

Name	Type	IsNullable	Length
COUNTY	esriFieldTypeString	TRUE	24
STATE	esriFieldTypeString	TRUE	2
COUNTRY	esriFieldTypeString	TRUE	40
POSTAL_CODE	esriFieldTypeString	TRUE	10
ZIP_PLUS_4	esriFieldTypeString	TRUE	4
POSTAL_COMMUNITY_NAME	esriFieldTypeString	TRUE	50
NEIGHBORHOOD_COMMUNITY	esriFieldTypeString	TRUE	100
MSAG_COMMUNITY_NAME	esriFieldTypeString	TRUE	50
ADDITIONAL_CODE	esriFieldTypeString	TRUE	6
ADDITIONAL_LOCATION_INFORMATION	esriFieldTypeString	TRUE	255
MILEPOST	esriFieldTypeString	TRUE	150
ESN	esriFieldTypeString	TRUE	10
ADDITIONAL_DATA_URI	esriFieldTypeString	TRUE	254

**Table 6: Alias Data Model**

Name	Type	IsNullable	Length
OBJECTID	esriFieldTypeOID	FALSE	4
SOURCE_OF_DATA	esriFieldTypeString	TRUE	75
DATE_UPDATED	esriFieldTypeDate	TRUE	8
EFFECTIVE_DATE	esriFieldTypeDate	TRUE	8
EXPIRATION_DATE	esriFieldTypeDate	TRUE	8
ALIAS_UNIQUE_ID	esriFieldTypeString	TRUE	100
ROAD_CENTERLINE_UNIQUE_ID	esriFieldTypeString	TRUE	100
ALIAS_STREET_NAME_PRE_MODIFIER	esriFieldTypeString	TRUE	15
ALIAS_STREET_NAME_PRE_DIRECTIONAL	esriFieldTypeString	TRUE	9
ALIAS_STREET_NAME_PRE_TYPE	esriFieldTypeString	TRUE	25
ALIAS_STREET_NAME_PRE_TYPE_SEPARATOR	esriFieldTypeString	TRUE	20
ALIAS_STREET_NAME	esriFieldTypeString	TRUE	75
ALIAS_STREET_NAME_POST_TYPE	esriFieldTypeString	TRUE	15

Name	Type	IsNullable	Length
ALIAS_STREET_NAME_POST_DIRECTIONAL	esriFieldTypeString	TRUE	9
ALIAS_STREET_NAME_POST_MODIFIER	esriFieldTypeString	TRUE	25

**Table 7: Boundary Data Model**

Name	Type	IsNullable	Length
OBJECTID	esriFieldTypeOID	FALSE	4
SHAPE	esriFieldTypeGeometry	TRUE	0
SHAPE_Length	esriFieldTypeDouble	TRUE	8
SHAPE_Area	esriFieldTypeDouble	TRUE	8
SOURCE_OF_DATA	esriFieldTypeString	TRUE	75
EFFECTIVE_DATE	esriFieldTypeDate	TRUE	8
EXPIRATION_DATE	esriFieldTypeDate	TRUE	8
DATE_UPDATED	esriFieldTypeDate	TRUE	8
EMERGENCY_SERVICE_UNIQUE_ID	esriFieldTypeString	TRUE	100
AGENCY_ID	esriFieldTypeString	TRUE	100
ROUTE_URI	esriFieldTypeString	TRUE	254
SERVICE_URN	esriFieldTypeString	TRUE	50
SERVICE_NUMBER	esriFieldTypeString	TRUE	50
AGENCY_VCARD_URI	esriFieldTypeString	TRUE	254
DISPLAY_NAME	esriFieldTypeString	TRUE	60

**Table 8: Road Data Model**

Name2	Type	IsNullable	Length	AliasName	ModelName
OBJECTID	esriFieldTypeOID	FALSE	4	OBJECTID	OBJECTID
SHAPE	esriFieldTypeGeometry	TRUE	0		SHAPE
SHAPE_Length	esriFieldTypeDouble	TRUE	8		SHAPE_Length
SOURCE_OF_DATA	esriFieldTypeString	TRUE	50	SOURCE OF DATA	SOURCE_OF_DATA

Name2	Type	IsNullable	Length	AliasName	ModelName
EFFECTIVE_DATE	esriFieldTypeDate	TRUE	8	EFFECTIVE DATE EXPIRATION DATE DATE UPDATED	EFFECTIVE_DATE
EXPIRATION_DATE	esriFieldTypeDate	TRUE	8	EXPIRATION DATE	EXPIRATION_DATE
DATE_UPDATED	esriFieldTypeDate	TRUE	8	DATE UPDATED	DATE_UPDATED
ROAD_CENTERLINE_UNIQUE_ID	esriFieldTypeString	TRUE	100	ROAD CENTERLINE UNIQUE ID	ROAD_CENTERLINE_UNIQUE_ID
ROAD_CLASS	esriFieldTypeString	TRUE	15	ROAD CLASS	ROAD_CLASS
STREET_NAME_PRE_MODIFIER	esriFieldTypeString	TRUE	30	STREET NAME PRE MODIFIER	STREET_NAME_PRE_MODIFIER
STREET_NAME_PRE_DIRECTIONAL	esriFieldTypeString	TRUE	12	STREET NAME PRE DIRECTIONAL	STREET_NAME_PRE_DIRECTIONAL
STREET_NAME_PRE_TYPE	esriFieldTypeString	TRUE	30	STREET NAME PRE TYPE	STREET_NAME_PRE_TYPE
STREET_NAME_PRE_TYPE_SEPARATOR	esriFieldTypeString	TRUE	30	STREET NAME PRE TYPE SEPARATOR	STREET_NAME_PRE_TYPE_SEPARATOR
STREET_NAME	esriFieldTypeString	TRUE	75	STREET NAME	STREET_NAME
STREET_NAME_POST_TYPE	esriFieldTypeString	TRUE	30	STREET NAME POST TYPE	STREET_NAME_POST_TYPE
STREET_NAME_POST_DIRECTIONAL	esriFieldTypeString	TRUE	12	STREET NAME POST DIRECTIONAL	STREET_NAME_POST_DIRECTIONAL
STREET_NAME_POST_MODIFIER	esriFieldTypeString	TRUE	30	STREET NAME POST MODIFIER	STREET_NAME_POST_MODIFIER
LEFT_ADDRESS_NUMBER_PREFIX	esriFieldTypeString	TRUE	15	LEFT ADDRESS NUMBER PREFIX	LEFT_ADDRESS_NUMBER_PREFIX
LEFT_FROM_ADDRESS	esriFieldTypeInteger	TRUE	0	LEFT FROM ADDRESS	LEFT_FROM_ADDRESS
LEFT_TO_ADDRESS	esriFieldTypeInteger	TRUE	0	LEFT TO ADDRESS	LEFT_TO_ADDRESS
LEFT_ADDRESS_NUMBER_SUFFIX	esriFieldTypeString	TRUE	15	LEFT ADDRESS NUMBER SUFFIX	LEFT_ADDRESS_NUMBER_SUFFIX
PARITY_LEFT	esriFieldTypeString	TRUE	1	PARITY LEFT	PARITY_LEFT
RIGHT_ADDRESS_NUMBER_PREFIX	esriFieldTypeString	TRUE	15	RIGHT ADDRESS NUMBER PREFIX	RIGHT_ADDRESS_NUMBER_PREFIX
RIGHT_FROM_ADDRESS	esriFieldTypeInteger	TRUE	0	RIGHT FROM ADDRESS	RIGHT_FROM_ADDRESS
RIGHT_TO_ADDRESS	esriFieldTypeInteger	TRUE	0	RIGHT TO ADDRESS	RIGHT_TO_ADDRESS
RIGHT_ADDRESS_NUMBER_SUFFIX	esriFieldTypeString	TRUE	15	RIGHT ADDRESS NUMBER SUFFIX	RIGHT_ADDRESS_NUMBER_SUFFIX
PARITY_RIGHT	esriFieldTypeString	TRUE	1	PARITY RIGHT	PARITY_RIGHT
INCORPORATED_MUNICIPALITY_LEFT	esriFieldTypeString	TRUE	100	INCORPORATED MUNICIPALITY LEFT	INCORPORATED_MUNICIPALITY_LEFT
INCORPORATED_MUNICIPALITY_RIGHT	esriFieldTypeString	TRUE	100	INCORPORATED MUNICIPALITY RIGHT	INCORPORATED_MUNICIPALITY_RIGHT
UNINCORPORATED_COMMUNITY_LEFT	esriFieldTypeString	TRUE	100	UNINCORPORATED COMMUNITY LEFT	UNINCORPORATED_COMMUNITY_LEFT
UNINCORPORATED_COMMUNITY_RIGHT	esriFieldTypeString	TRUE	100	UNINCORPORATED COMMUNITY RIGHT	UNINCORPORATED_COMMUNITY_RIGHT
COUNTY_LEFT	esriFieldTypeString	TRUE	40	COUNTY LEFT	COUNTY_LEFT

Name2	Type	IsNullable	Length	AliasName	ModelName
COUNTY_RIGHT	esriFieldTypeString	TRUE	40	COUNTY RIGHT	COUNTY_RIGHT
STATE_LEFT	esriFieldTypeString	TRUE	2	STATE LEFT	STATE_LEFT
STATE_RIGHT	esriFieldTypeString	TRUE	2	STATE RIGHT	STATE_RIGHT
COUNTRY_LEFT	esriFieldTypeString	TRUE	2	COUNTRY LEFT	COUNTRY_LEFT
COUNTRY_RIGHT	esriFieldTypeString	TRUE	2	COUNTRY RIGHT	COUNTRY_RIGHT
POSTAL_CODE_LEFT	esriFieldTypeString	TRUE	10	POSTAL CODE LEFT	POSTAL_CODE_LEFT
POSTAL_CODE_RIGHT	esriFieldTypeString	TRUE	10	POSTAL CODE RIGHT	POSTAL_CODE_RIGHT
POSTAL_COMMUNITY_NAME_LEFT	esriFieldTypeString	TRUE	50	POSTAL COMMUNITY NAME LEFT	POSTAL_COMMUNITY_NAME_LEFT
POSTAL_COMMUNITY_NAME_RIGHT	esriFieldTypeString	TRUE	50	POSTAL COMMUNITY NAME RIGHT	POSTAL_COMMUNITY_NAME_RIGHT
NEIGHBORHOOD_COMMUNITY_LEFT	esriFieldTypeString	TRUE	50	NEIGHBORHOOD COMMUNITY LEFT	NEIGHBORHOOD_COMMUNITY_LEFT
NEIGHBORHOOD_COMMUNITY_RIGHT	esriFieldTypeString	TRUE	50	NEIGHBORHOOD COMMUNITY RIGHT	NEIGHBORHOOD_COMMUNITY_RIGHT
MSAG_COMMUNITY_NAME_LEFT	esriFieldTypeString	TRUE	50	MSAG COMMUNITY NAME LEFT	MSAG_COMMUNITY_NAME_LEFT
MSAG_COMMUNITY_NAME_RIGHT	esriFieldTypeString	TRUE	50	MSAG COMMUNITY NAME RIGHT	MSAG_COMMUNITY_NAME_RIGHT
ESN_LEFT	esriFieldTypeString	TRUE	10	ESN LEFT	ESN_LEFT
ESN_RIGHT	esriFieldTypeString	TRUE	10	ESN RIGHT	ESN_RIGHT
ONE_WAY	esriFieldTypeString	TRUE	2	ONE-WAY	ONE_WAY
SPEED_LIMIT	esriFieldTypeSmallInteger	TRUE	2	SPEED LIMIT	SPEED_LIMIT
ADDITIONAL_CODE_LEFT	esriFieldTypeString	TRUE	6	ADDITIONAL CODE LEFT	ADDITIONAL_CODE_LEFT
ADDITIONAL_CODE_RIGHT	esriFieldTypeString	TRUE	6	ADDITIONAL CODE RIGHT	ADDITIONAL_CODE_RIGHT



Attachment C: Requirements Compliance Summary

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
3.1.1.1						
3.1.1.2						
3.1.1.3						
3.2						
3.3						
3.5						
4.1.1						
4.1.2						
4.2						
4.3.1						
4.3.2						
4.3.3						
4.3.4						
4.3.5						
4.3.6						
4.3.7						
4.3.8						
4.3.9						
4.3.10						
4.3.11						
4.3.12						
4.3.13						
4.4.1						
4.4.2						
4.5						
4.6.1						
4.7						
4.7.1.1						
4.7.1.2						
4.7.2						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
4.7.3.1						
4.7.3.2						
4.7.4.1						
4.8.1						
4.8.2						
4.8.3						
4.8.4						
4.8.5						
4.8.6						
4.8.1.1						
4.8.1.2						
4.9.1						
4.9.2						
4.9.1.1						
4.9.1.2						
4.9.1.3						
4.9.1.4						
4.9.2						
4.9.3.1						
4.9.3.2						
4.9.4.1						
4.9.4.2						
4.9.5.1						
4.9.5.2						
4.9.5.3						
4.9.6.1						
4.9.6.2						
4.9.7						
4.9.8						
4.9.9						
4.9.10						
4.9.11						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
4.9.12						
4.9.13.1						
4.9.13.2						
4.9.13.3						
4.9.13.4						
4.9.13.5						
4.9.13.6						
4.9.14.1						
4.9.14.2						
4.9.14.3						
4.10						
4.10.1.1						
4.10.1.2						
4.10.1.3						
4.10.1.4						
4.10.1.5						
4.10.1.6						
4.10.1.7						
4.10.1.8						
4.10.1.9						
4.10.1.10						
4.10.1.11						
4.10.1.12						
4.10.2.1						
4.10.2.2						
4.10.2.3						
4.10.2.4						
4.10.2.5						
4.10.2.6						
4.10.2.7						
4.10.3.1						
4.10.3.2						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
4.10.3.3						
4.10.3.4						
4.10.3.5						
4.10.3.6						
4.10.3.7						
4.10.3.8						
4.10.3.9						
4.10.3.10						
4.10.3.11						
4.10.3.12						
4.10.3.13						
4.10.3.14						
4.10.4.1						
4.10.4.2						
4.10.4.3						
4.10.4.4						
4.10.4.5						
4.10.4.6						
4.10.4.7						
4.10.4.8						
4.10.4.8.1						
4.10.4.8.2						
4.10.4.8.3						
4.10.4.8.4						
4.10.4.8.5						
4.10.4.8.6						
4.10.4.8.7						
4.10.4.8.8						
4.10.4.8.9						
4.10.4.8.10						
4.10.4.8.11						
4.10.4.8.12						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
4.10.4.8.13						
4.10.4.8.14						
4.10.4.8.15						
4.10.4.8.16						
4.10.4.8.17						
4.10.4.8.18						
4.10.4.8.19						
4.10.4.8.20						
4.10.4.8.21						
4.10.5.1						
4.10.5.2						
4.10.5.3						
4.10.5.4						
4.10.5.5						
4.10.5.6						
4.10.5.7						
4.10.5.8						
4.10.5.9						
4.10.5.10						
4.10.5.11						
4.10.5.12						
4.10.6.1						
4.10.6.2						
4.10.6.3						
4.10.6.4						
4.10.6.5						
4.10.7.1						
4.10.7.2						
4.10.7.3						
4.10.7.4						
4.10.8.1						
4.10.8.2						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
4.10.9						
4.10.10.1						
4.10.10.2						
4.10.10.3						
4.10.10.4						
4.10.10.5						
4.10.10.6						
4.10.10.7						
4.10.11.1						
4.10.11.2						
4.10.12.1						
4.10.12.2						
4.10.13						
4.11.1						
4.11.2.1						
4.11.2.3						
4.11.2.4						
4.11.2.5						
4.11.2.6						
4.11.2.7						
4.11.2.8						
4.11.2.9						
4.11.2.10						
4.11.3						
4.11.4.1						
4.11.4.2						
4.11.4.3						
4.11.4.4						
4.11.4.5						
4.11.5						
4.11.6						
4.11.7						

Requirement	Understood	Complies	Complies Partially	Complies with Future Capability	Does Not Comply	Response Provided
4.12.1						
4.12.2						
4.12.3						
4.12.4						
5.1						
5.2						
5.3						
5.4						
5.5						
6.1						
6.2						
6.3						
6.4						
6.5						
7.1						
7.2						
8						
9.1.1						
9.1.2						
9.2.1						
9.2.2						
9.2.3						
9.2.4						
10						

**Attachment D: Sample of Required 10-Digit Transfers**

<b>PSAP</b>	<b>County</b>	<b>City</b>	<b>ST</b>	<b>ZIP</b>	<b>NPA-NXX</b>
Maryland State Police Rockville	Montgomery	Rockville	MD	20854	301-424
Maryland Transportation Authority Police	Montgomery	Baltimore	MD	21224	410-537
MNCPPC – Police, Montgomery Division	Montgomery	Silver Spring	MD	20906	301-949
Washington Metropolitan Area Transit Authority	Montgomery	College Park	MD	20740	301-474
NSA - Bethesda	Montgomery	Bethesda	MD	20889	301-295
NSA - Carderock	Montgomery	Bethesda	MD	20817	301-227
U.S. Park Police	Montgomery & Prince George's				202-610
Fort Belvoir	Arlington				
Joint Base Myer-Henderson Hall	Arlington	Arlington	VA	22214	703-979, 703-614, 571-483
Marine Corp Base Quantico	Prince William	Quantico	VA	22134	703-784
Pentagon	Arlington	Washington (in Arlington)	DC	20301	703-545
Joint Base Andrews	Prince George's				
Fort George G. Meade	Anne Arundel	Fort Meade	MD	20755	301-677
Fort Detrick	Frederick	Frederick	MD	21702	301-619
Indian Head Naval Warfare Center Study Area**	Charles	Indian Head	MD	20640	301-744
Joint Base Anacostia-Bolling**	DC				
Fort McNair Army Base**	DC				
Coast Guard Headquarters**	DC				
Marine Barracks Marine Corp Base**	DC				
Naval Research Laboratory**	DC				
Navy Yard**	DC				
George Mason University	Fairfax	Fairfax	VA	22030	703-993
Bowie State University	Prince George's	Bowie	MD	20715	301-860
University of Maryland, College Park	Prince George's	College Park	MD	20740	301-405
Hood College	Frederick	Frederick	MD	21701	301-663
Mount St. Mary's University	Frederick	Emmitsburg	MD	21727	301-447
Maryland State Police College Park	Prince George's	College Park	MD	20740	301-345



PSAP	County	City	ST	ZIP	NPA-NXX
Maryland State Police Frederick	Frederick	Frederick	MD	21707	301-663
Maryland State Police Forestville	Prince George's	Forestville	MD	20747	301-568
Maryland State Police La Plata	Charles	La Plata	MD	20646	410-753

\*\* Denotes calls are answered at the Navy Yard Emergency Dispatch Center primarily and at Naval Air Station Oceana as a backup