Systems Requirements Document (SRD)

Global Public Safety Communications (GPSC)

Public Safety Answering Point (PSAP), Public Safety IP Network (PSInet) & Next Generation Core Services (NGCS)

Submitted by: Jon Marcy (NetMaker Communications LLC)
Lead Engineer
DoD Office of Global Public Safety Communications Modernization

Approved and Released by: John Holloway
Director
DoD Office of Global Public Safety Communications Modernization

HOLLOWAY.JOHN.EGGLESTON.JR.1014491119

Digitally signed by HOLLOWAY.JOHN.EGGLESTON.JR.1014491119
Date: 2023.11.27 05:46:29 -05'00'

Version 0.5.0

DOCUMENT REVISION HISTORY

Project Name: Public Safety IP Network (PSInet)

Document Status (Draft):

Change Request#	Document Version	Approval Dates	Modified By	Section, Page(s) & Text Revised
NA	0.1.0	NA	F Black	Initial Draft
NA	0.2.0	NA	L Curling	All – Complete re-map outline to match Numbering Scheme. Add NS# to sections.
NA	0.3.0	NA	L Curling	All – Reformat to SRD format.
NA	0.4.0	NA	L Curling	All – Reformat to SRD format.
NA	0.4.2	NA	L Curling	All – Incorporate JITC feedback
NA	0.4.3	NA	M. Fowler	All – Edit, proof and format version 0.4.2
NA	0.4.4	NA	L Curling	All – Incorporate round 2 JITC feedback add PSAP
NA	0.4.5	NA	J. Marcy	Added Section 4.7.4 Computer Aided Dispatch
NA	0.4.6	NA	L. Curling	All- Incorporate field comments
NA	0.4.7	NA	L. Curling	All- Requirement Numbering
NA	0.4.8	NA	L. Curling	All- incorporate PSAP/ECC change & Final Review
NA	0.5.0	NA	L. Curling	FINAL

TABLE OF CONTENTS
Table of Contents

1 SCOPE 1

1.1 SYSTEM IDENTIFICATION 2
1.2 SYSTEM OVERVIEW 3
1.2.1 Location Information Service (LIS) / Geographic Information System (GIS) 3
1.2.2 Boundary Cloud Access Point (BCAP) / Voice Cloud Access Point (VCAP) 3
1.2.3 NGCS 4
1.2.4 MPG 4
1.2.4 Mission Partner Voice Enclave 4
1.2.6 PSAP/ECC 4

2 APPLICABLE DOCUMENTS 5

2.1 GENERAL 5
2.2 COMPANION DOCUMENT 5

3 COMMON PROTOCOL REQUIREMENTS 5

3.1 SYSTEM INTERNAL INTERFACE REQUIREMENTS 5
3.1.1 HTTP Enabled Location Delivery (HELD) 5
3.1.2 Location-to Service Translation (LoST) 8
3.1.4 IPV6 10
3.1.5 SIP 14
3.2 SYSTEM AVAILABILITY 16

4 FUNCTIONAL ELEMENT REQUIREMENTS 17

4.1 CSPR 17
4.1.1 CSPR Interface Support Requirements 17
4.2 PSPR 17
4.2.1 Summary 17
4.2.2 Standards 18
4.2.3 Set of requirements 18
4.3 LOCATION INFORMATION SERVER (LIS) 20
4.3.1 Summary 20
4.3.2 Set of requirements 20
4.4 SI/GIS 22
4.4.1 GIS Datastore Summary 22
4.4.2 Set of requirements 22
4.4.3 SI Summary 23
4.4.4 Set of requirements 23
4.5 PSAP/ECC 23
4.5.1 SIP Call interface 23
4.5.2 Test Calls 24
4.5.3 Call Diversion 25
4.5.4 Bridge Interface 26
4.5.5 Computer Aided Dispatch (CAD) / Unified CAD (UCAD) 26
4.5.6 Logging Service 27
4.5.7 Time Interface 27
4.5.8 GIS27
4.6 SBC 28
4.6.1 SBC Requirements 28
4.7 SC/SS 29
4.7.1 SC Requirements 29

5 APPENDIX A - ACRONYM GLOSSARY 30

6 APPENDIX B - SUPPORTED STANDARDS 33

7 APPENDIX C – CALL FLOW DIAGRAMS 39

8 APPENDIX D – FUNCTIONAL REQUIREMENTS DOCUMENT (FRD) FOR PUBLIC SAFETY COMMUNICATIONS, VOLUME 1 41

Appendix D1 – Architecture 41
Appendix D2 – Call Flow 44
Appendix D3 – Service Creation 46
Appendix D4 – Basic Services Data Associated with a Call 47
Appendix D5 – Event Notification 48
Appendix D6 – Security 49
Appendix D7 – Service Management 50
Appendix D8 – Roles and Responsibilities 51
Appendix D9 – Profile Minimal-Profile Definition 52
Appendix D10 – Call Handling/CAD Event Creation 53
Appendix D11 – Dispatch Support 56
Appendix D12 – Resource Management 60
Appendix D13 – Call Incident/Event Management 63
Appendix D14 – Supplemental Resource Request Tracking 65
Appendix D15 – Incident Disposition 66
Appendix D16 – Business Function/CAD Administration 67
Appendix D17 – System Functions 70
Appendix D18 – Reporting and Monitoring 72
Appendix D19 – Interfaces 73
Appendix D20 – Common Operational Picture (COP) 77
Appendix D21 – GIS/CAD Mapping Integration 77
Appendix D22 – 911 Telephony Integration and Data Standards 77
Appendix D23 – References 78
Appendix D24 – Acronyms and Definitions 79

Table of Figures

FIGURE 1. - DOD PSC OV-1 FIELDING 2023-2026 2

FIGURE 2. - DOD PSC OV-1 FIELDING 2027 2

FIGURE 3. - SIP LOCATION CAPABLE END INSTRUMENT 39

FIGURE 4. - LEGACY ANALOG/DIGITAL/SIP EI LOCATION INSERTED BY LSC . 40

FIGURE 5. - LOCATION INSERTED BY SBC IN RSC ARCHITECTURE 40

1 SCOPE

This document serves as the technical foundation and provides extensive external technical references for the Joint Interoperability Test Command (JITC) to build test plans and certify systems for the DoD Unified Capabilities Approved Products List (APL) in accordance with the DODI 8100.04. This document is to be publicly releasable.

This document contains the text-based detailed requirements for the delivery of the Next Generation Core Services (NGCS) elements as well as the Public Safety IP Network (PSInet) for Global Public Safety Communications (GPSC). The final system architecture utilizes the standardized structure and design of the National Emergency Numbering Association (NENA) i3 framework to allow interoperability between the Department of Defense (DoD) PSInet and commercial emergency services IP networks (ESInet). Refer to the NextGen 9-1-1 Functional Requirements Document (FRD) for additional framework guidance.

This document is intended to be updated regularly to enable the DoD to keep pace with industry standards, requirements, and Information and Communications Technology (ICT) and Cyber-Supply Chain Risk Management (C-SCRM) best practices. Updates shall ensure continual interoperability and backwards compatibility with evolving NENA i3 standards. Maintaining full interoperability is required to guarantee call delivery to commercial Public Safety Answering Points (PSAP)/Emergency Communications Centers (ECC) via the Mission Partner Gateways (MPG).

The scope of this Systems Requirements Document (SRD) is to detail the requirements, specifications, systems, and interface requirements for all NGCS functional elements supporting the DoD PSInet for the GPSC i3-based ESInet. It details the specifications and behavior for all software products and services, hardware, and networks operating within the PSInet. Additionally, detailed messaging definition for the PSInet is described as well as the interconnection between PSAP/ECCs and the PSInet, in addition to State/Municipal ESInet-to-PSInet interconnections. **Figures 1 and 2: DOD GPSC OV-1** provide an operational overview of the NG9-1-1 ecosystem out to 2027.

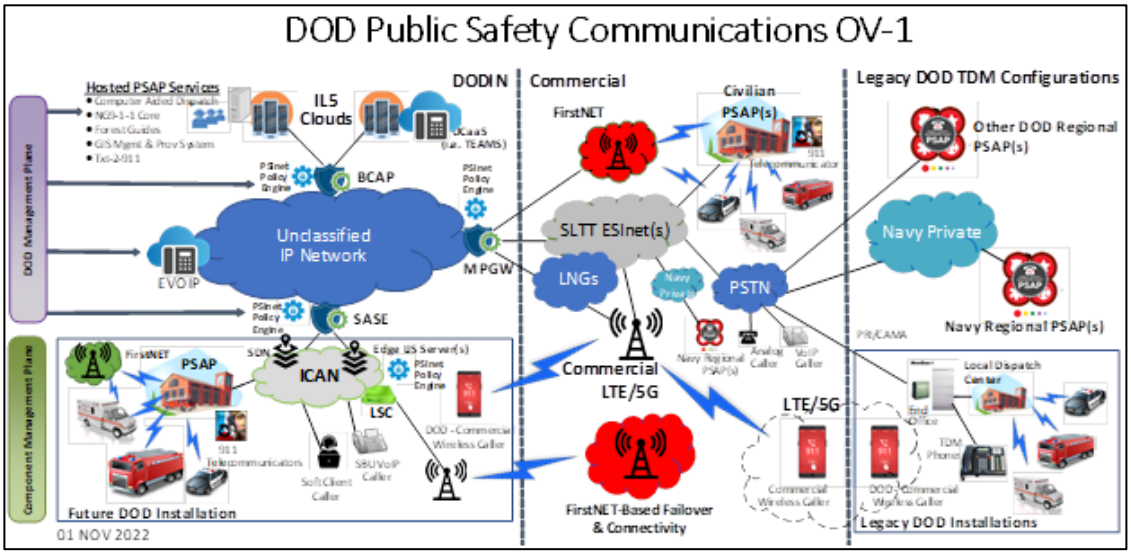
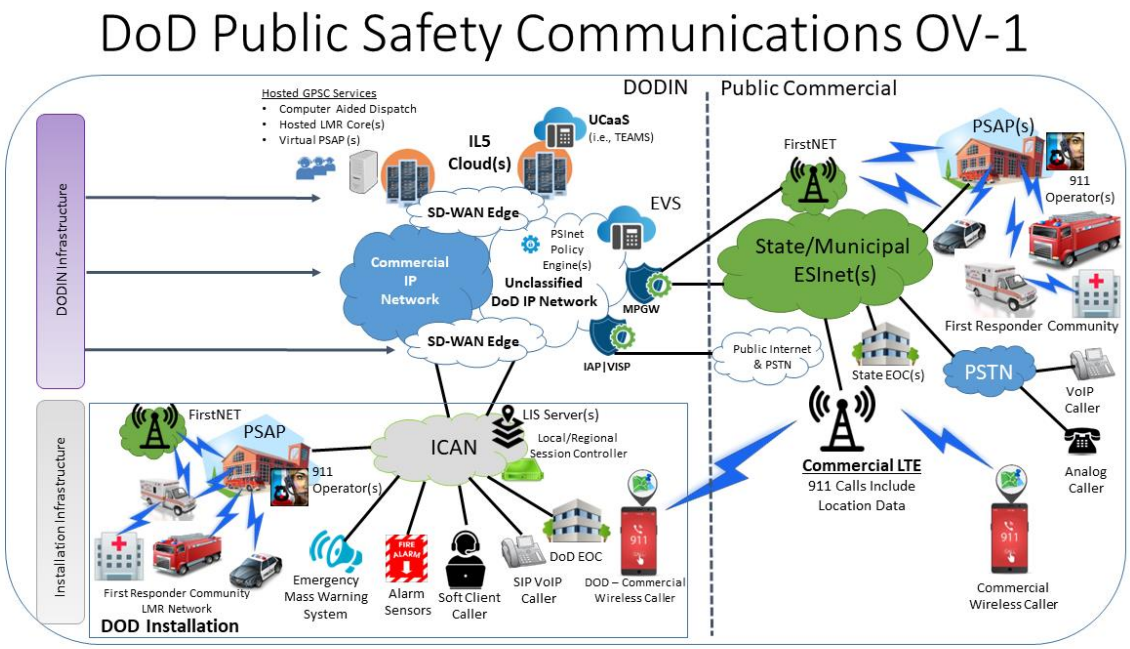


Figure 1. - DoD PSC OV-1 Fielding 2023-2026



1

Figure 2. - DoD PSC OV-1 Fielding 2027

1.1 System Identification

The Next Generation 9-1-1 system is comprised of the following subsystems:

1. Public Safety IP Network and associated NexGen core services.
2. Public Safety Answering Point and associated call handling and Computer Aided Dispatch systems.
3. Location Information Services and associated Geospatial Information Systems.

1.2 System Overview

The scope of this system comprises the PSInet, NGCS, and PSAP/ECC interconnections. This system is composed of a series of interconnected subsystems. These subsystems often have overlapping technologies that are required for interoperability.

The PSInet shall consist of a virtual IP network—shared with the unclassified voice network—established on the DISA-managed global unclassified Multi-Protocol Label Switching (MPLS) network. Based on the establishment of an MPLS Virtual Routing and Forwarding (VRF) instance on the unclassified network, the PSInet shall consist of shared, geographically positioned policy-engine servers and the associated Session Border Controller (SBC) cybersecurity solutions of the Enterprise Voice Services (EVS) initiative. This configuration shall support the internal routing of Session Initiation Protocol (SIP)-based 9-1-1 calls to DoD PSAP/ECC facilities as well as the ingress and egress of SIP-based 9-1-1 calls between the unclassified Voice over IP (VoIP) soft-switch backbone, MPG, and the PSInet.

1.2.1 Location Information Service (LIS) / Geographic Information System (GIS)

The establishment of LIS capabilities paired with accurate GIS data in the NENA i3 recommended format is a key factor of NG9-1-1. The DOD IP network shall be configured to provide locations of endpoints (i.e., calling devices). An LIS can provide Location-by-Reference or Location-by-Value. If employing Location-by-Value, the value can be in either geo (latitude/longitude) or civic (street address) forms. LIS capabilities shall be established as part of the DOD VoIP framework and managed by the Components responsible for installation VoIP deployments and sustainment. IP voice capabilities shall include the ability to query an LIS and insert the received location information into the SIP header of a 9-1-1 call before the call is routed out of the originating voice enclave. Additional architectural and technical details are found in the Next Generation 9-1-1 Technical Architecture Document (NG9-1-1 TAD).

1.2.2 Boundary Cloud Access Point (BCAP) / Voice Cloud Access Point (VCAP)

In support of any FedRAMP-approved hosted software employed to deliver PSInet, NGCS, and PSAP/ECC capabilities, the software shall obtain Impact Level 5 (IL5) Provisional Authority (PA) to operate, as well as a valid Authorization to Operate (ATO) to connect to the DISA unclassified BCAP and/or VCAP. All SIP-based network traffic (i.e., signaling and media) shall traverse the VCAP, while all other TCP/IP-related network traffic shall traverse the BCAP. The BCAP is currently planned to retire in 2026 with the architecture transitioning to Software Defined Wide Area Networking (SD-WAN).

1.2.3 NGCS

The NGCS and PSInet make up the core call-routing subsystem responsible for ensuring calls routed to the correct PSAP/ECC. Unlike the commercial ESInets, the DISA shall establish a global PSInet to support all DoD users.

In the system core, the critical functional elements are: the SBC, Core Session Policy Router (CSPR), Public Safety Policy Router (PSPR). The PSPR, as a product, shall incorporation the following NENA i3 functions: Emergency Call Routing Function (ECRF), and Location Validation Function (LVF).

1.2.4 MPG

The MPG is the security boundary responsible for interconnecting the DoD PSInet to commercial ESInets. The MPG consists of the following functional elements: Firewalls, Intrusion Detection/Prevention Systems and SBCs. The interface between the MPG and ESInets will need individually designed to ensure proper call handling for both wireline and wireless calls. This is due to the fact every state has a potentially unique ESInet configuration. Wireless emergency services call which originates from a location serviced by a DoD PSAP/ECC will be routed from the commercial wireless carrier to the closest state ESInet. The caller's location will be identified by a dynamic location reference in the call header. The servicing PSAP/ECC will de-reference the location reference by querying the location server in the carrier network to provide a dispatchable location.

1.2.4 Mission Partner Voice Enclave

In the mission-partner voice enclave, the critical functional elements to support NG9-1-1 are the end instrument (EI), Session Controller (SC), Location Information Services (LIS), and Session Border Controller (SBC).

1.2.6 PSAP/ECC

The PSAP/ECC as defined in this document shall be an NG9-1-1 or legacy E9-1-1 emergency services answer-and-dispatch center located on a DoD facility in compliance with U.S. Federal laws.

Within the United States, 9-1-1 calls may be routed to a DoD Emergency Response Center (DoD PSAP/ECC) or to a civil PSAP. The emergency-services network that handles DoD and PSTN 911 calls may be TDM-based or IP-based.

Outside of the United States, 9-1-1 calls may be routed to a DoD PSAP/ECC (if one exists at the DoD location). If no DoD PSAP/ECC exists, 9-1-1 calls shall transit the PSInet and exit via the MPG for delivery to the civil PSAP/ECC serving the caller location based on local policy.

2 APPLICABLE DOCUMENTS

2.1 General

Documents listed in this section are specified in sections 3, 4, or 5 of this SRD. This section does not include documents cited in other sections of this specification or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, readers are cautioned that they should meet all specified requirements of documents cited in sections 3, 4, or 5 of this specification, whether they are listed in this section. The documents with links relevant at the time of publication are included in Appendix B.

2.2 Companion document

The SRD is meant to be used in conjunction with the Next Generation 9-1-1 (NG9-1-1) FRD serving as the Public Safety framework.

3 COMMON PROTOCOL REQUIREMENTS

3.1 System Internal Interface Requirements

3.1.1 HTTP Enabled Location Delivery (HELD)

PSI-000180 [Required: GIS, LIS, SBC, PSPR] The product shall support HELD is defined in RFC 5985 and RFC 7840. HELD provides a non-SIP location delivery.

PSI-000190 [Required: GIS, LIS, SBC, PSPR] When responding to HELD, the product shall support Presence Information Data Format - Location Object (PIDF-LO) as described in IETF RFC 4119 and updated by IETF RFC 5139 and IETF RFC 5491.

PSI-000200 [Required: GIS, LIS, SBC, PSPR] All geodetic data shall use WORLD GEODETIC SYSTEM 1984 (WGS84) as the datum.

PSI-000210 [Required: GIS, LIS, SBC, PSPR] The representation of the location object within the Presence Information Data Format document shall utilize the <tuple> element as defined in IETF RFC 4119.

PSI-000220 [Required: GIS, LIS, SBC, PSPR] A <geopriv> element shall describe a discrete location. Where a discrete location can be uniquely described in more than one way, each location description shall reside in a separate <tuple> element with only one <geopriv> element per <tuple>.

PSI-000230 [Required: GIS, LIS, SBC, PSPR] Providing more than one location element in a single <location-info> element should only be used to represent a compound location referring to the same place. For example, a geodetic location describing a point, and a civic location indicating the floor in a building at that point.

PSI-000240 [Required: GIS, LIS, SBC, PSPR] Elements evaluating a PIDF-LO shall respect the order of <geopriv> elements in the presence document received.

3.1.1.1 PIDF-LO

PIDF-LO is a core element for location data in an emergency services call containing the geographical location information describes a physical position in the world.

PSI-000250 [Required: GIS, LIS, SBC, PSPR] The product shall support the base function of PIDF-LO as covered in RFC 4119 updated by RFC 5139. The GEOPRIV PIDF-LO is covered in RFC 4119 updated by RFC 5491.

PSI-000270 [Required: GIS, LIS, SBC, PSPR] The product shall support the baseline PIDF usage of the GEOPRIV element in RFC 5139 Sec2.1.

PSI-000280 [Required: GIS, LIS, SBC, PSPR] The product shall support the location-info as defined in RFC 5139 sec 2.1.1.

PSI-000290 [Required: GIS, LIS, SBC, PSPR] The product may support the method as defined in RFC 5139 sec 2.1.3.

PSI-000300 [Required: GIS, LIS, SBC, PSPR] The product may support the provided-by as defined in RFC 5139 sec 2.1.4.

PSI-000310 [Conditional: GIS, LIS, SBC, PSPR] Where civic address data is used the function shall support the xml schema in RFC 5139 sec 4.

The following is an example of a Civic Address XML schema:

```
<?xml version="1.0"?>
  <xs:schema
   targetNamespace="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
   xmlns:xml="http://www.w3.org/XML/1998/namespace"
   elementFormDefault="qualified" attributeFormDefault="unqualified">

   <xs:import namespace="http://www.w3.org/XML/1998/namespace"
        schemaLocation="http://www.w3.org/2001/xml.xsd"/>

   <xs:simpleType name="iso3166a2">
    <xs:restriction base="xs:token">
     <xs:pattern value="[A-Z]{2}"/>
    </xs:restriction>
   </xs:simpleType>

   <xs:complexType name="caType">
    <xs:simpleContent>
     <xs:extension base="xs:token">
      <xs:attribute ref="xml:lang" use="optional"/>
     </xs:extension>
    </xs:simpleContent>
   </xs:complexType>
   <xs:element name="civicAddress" type="ca:civicAddress"/>
   <xs:complexType name="civicAddress">
    <xs:sequence>
     <xs:element name="country" type="ca:iso3166a2" minOccurs="0"/>
     <xs:element name="A1" type="ca:caType" minOccurs="0"/>
     <xs:element name="A2" type="ca:caType" minOccurs="0"/>
```

```
    <xs:element name="A3" type="ca:caType" minOccurs="0"/>
    <xs:element name="A4" type="ca:caType" minOccurs="0"/>
    <xs:element name="A5" type="ca:caType" minOccurs="0"/>
    <xs:element name="A6" type="ca:caType" minOccurs="0"/>
    <xs:element name="PRM" type="ca:caType" minOccurs="0"/>
    <xs:element name="PRD" type="ca:caType" minOccurs="0"/>
    <xs:element name="RD" type="ca:caType" minOccurs="0"/>
    <xs:element name="STS" type="ca:caType" minOccurs="0"/>
    <xs:element name="POD" type="ca:caType" minOccurs="0"/>
    <xs:element name="POM" type="ca:caType" minOccurs="0"/>
    <xs:element name="RDSEC" type="ca:caType" minOccurs="0"/>
    <xs:element name="RDBR" type="ca:caType" minOccurs="0"/>
    <xs:element name="RDSUBBR" type="ca:caType" minOccurs="0"/>
    <xs:element name="HNO" type="ca:caType" minOccurs="0"/>
    <xs:element name="HNS" type="ca:caType" minOccurs="0"/>
    <xs:element name="LMK" type="ca:caType" minOccurs="0"/>
    <xs:element name="LOC" type="ca:caType" minOccurs="0"/>
    <xs:element name="FLR" type="ca:caType" minOccurs="0"/>
    <xs:element name="NAM" type="ca:caType" minOccurs="0"/>
    <xs:element name="PC" type="ca:caType" minOccurs="0"/>
    <xs:element name="BLD" type="ca:caType" minOccurs="0"/>
    <xs:element name="UNIT" type="ca:caType" minOccurs="0"/>
    <xs:element name="ROOM" type="ca:caType" minOccurs="0"/>
    <xs:element name="SEAT" type="ca:caType" minOccurs="0"/>
    <xs:element name="PLC" type="xs:token" minOccurs="0"/>
    <xs:element name="PCN" type="ca:caType" minOccurs="0"/>
    <xs:element name="POBOX" type="ca:caType" minOccurs="0"/>
    <xs:element name="ADDCODE" type="ca:caType" minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax"
        minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>
 </xs:schema>
```

PSI-000320 [Required: GIS, LIS, SBC, PSPR] All functions shall prioritize geospatial (GeoShape) data as defined in RFC 5491 sec 5.

PSI-000330 [Required: GIS, LIS, SBC, PSPR] The product shall support both 2D and 3D geospatial formats.

The following is a sample XML schema for a 2D location point:

```
<presence xmlns="urn:ietf:params:xml:ns:pidf"
       xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
       xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
       xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
       xmlns:gml="http://www.opengis.net/gml"
       entity="pres:point2d@example.com">
  <dm:device id="point2d">
   <gp:geopriv>
    <gp:location-info>
     <gml:Point srsName="urn:ogc:def:crs:EPSG::4326">
      <gml:pos>-34.407 150.883</gml:pos>
     </gml:Point>
    </gp:location-info>
```

```
    <gp:usage-rules/>
    <gp:method>Wiremap</gp:method>
   </gp:geopriv>
   <dm:deviceID>mac:1234567890ab</dm:deviceID>
   <dm:timestamp>2007-06-22T20:57:29Z</dm:timestamp>
  </dm:device>
 </presence>
```

3.1.2 Location-to Service Translation (LoST)

LoST – Location-to-Service Translation – LoST (RFC5222) is a protocol designed specifically to request and convey location information to and from a LoST server. In NG9-1-1 it is used for location-based call routing.

PSI-000340 [Required: CSPR, PSPR] All SIP-based emergency calls pass location information either by value (PIDF-LO) or by reference (Location URI) plus a Service URN to an Emergency Services Routing Proxy (ESRP) to support routing of emergency calls.

PSI-000350 [Required: CSPR, PSPR] The CSPR shall process a LoST query to the PSPR when receiving an emergency call via a SIP INVITE.

PSI-000360 [Required: CSPR, PSPR] The CSPR shall pass the Service URN and location information via the LoST interface (as defined in IETF RFC 5222) to PSPR, which determines the next hop in routing a call to the requested service.

PSI-000370 [Conditional: CSPR, PSPR] If an element using LoST receives location by reference, it shall de-reference the URI to obtain the value prior to querying the LoST server. The LoST server does not accept location by reference.

PSI-000380 [Required: CSPR, PSPR] The PSPR shall the map the call's location information and requested Service URN to a "PSAP URI" by querying its data and then returning the URI provided. Using the returned URI and other information (time-of-day, PSAP/ECC state, etc.), the CSPR policy shall determine the appropriate routing URI. The LoST protocol (RFC 5222) allows civic location information to be returned in an XML format. The system shall support the XML schema in the RFC including the following service calls:

<findService> and <findServiceResponse>

<getServiceBoundary> and <getServiceBoundaryResponse>

<listServices> and <listServicesResponse>

<listServicesByLocation> and <listServicesByLocationResponse>

findService Request

PSI-000390 [Required: CSPR, PSPR] The product shall support “civic” and “geodetic-2d” profiles are baseline profiles defined in IETF RFC 5222, and emergency calls are expected to use only these profiles.

PSI-000400 [Optional: CSPR, PSPR] Conformant LoST servers may, but are not required to support any location profiles beyond these baseline profiles.

PSI-000410 [Required: CSPR, PSPR] The LoST interface shall allow a geo-location to be expressed as a point or one of several defined "shapes," such as circle, ellipse, arc band, or polygon.

PSI-000420 [Required: CSPR, PSPR] PSPR shall understands and handles all shapes in **PSI-000410**. The "service" element shall identify the service requested by the client.

PSI-000430 [Required: CSPR, PSPR] Valid service names shall be urn:service:sos or one of its sub-services for PSPR queries used by entities or devices for emergency calls.

PSI-000440 [Optional: CSPR, PSPR] PSPR implementations may support additional service names used internal to the PSInet dependent on the provisioning of service boundary layers in a geographical information system.

findService Response

PSI-000450 [Conditional: PSPR] A PSPR server may operate in recursive mode or iterative mode if the server being queried is not authoritative for the location supplied.

PSI-000460 [Required: PSPR] When recursion is used the PSPR shall initiate a query on behalf of the requestor that propagates through other PSPRs to an authoritative PSPR that returns the PSAP URI back through the intervening PSPRs to the requesting PSPR.

PSI-000470 [Required: PSPR] The use of iteration by the PSPR shall return a domain name of the next PSPR to contact.

PSI-000480 [Conditional:] The PSPR may operate in a recursive mode or an iterative mode, depending on local provisioning and the value of the 'recursive' attribute of the <findService> request. All PSPR implementations shall support both recursive and iterative modes.

PSI-000490 [Required: PSPR] When the PSPR successfully processes a LoST <findService> message, it shall return a LoST <findServiceResponse> message containing a <mapping> element that includes the "next hop" CSPR or PSAP URI in the <uri> element. If the PSPR cannot successfully process a LoST <findService> message, it shall return a LoST <errors> message indicating the nature of the error or a LoST <redirect> message indicating the PSPR that can process the <findService> message.

PSI-000500 [Required: PSPR] The <uri> returned shall specify either the next hop URI of the PSAP/ECC or the CSPR that is appropriate for the location sent in the query message. This shall be a globally routable URI with a scheme of sip for urn:service:sos. Some other service URNs may return values with HTTP/HTTPS schemes. LoST servers shall return SIPS and HTTPS URIs in addition to the SIP and HTTP (where appropriate) URIs.

PSI-000510 [Required: CSPR, PSPR] The *expires* attribute in the <mapping> element provides an PSPR with a way to control load, balancing it against the time required to completely implement a routing change when circumstances require. By increasing the expiration time, fewer queries to the server may be received if upstream LoST servers or clients implement caching. The product shall support a variable *expires*.

PSI-000520 [Required: CSPR, PSPR] The LoST response contains <via> elements in the <path> element that name the LoST servers visited to obtain the answer. Vias shall be returned to be compliant with IETF RFC 5222 and are essential for use in error resolution.

PSI-000530 [Required: CSPR, PSPR] The product shall support <displayName> element of the <mapping> response as a text string to indicate the serving agency(ies) for the location provided in the query. This information could be useful to PSAP/ECCs that query an PSPR.

PSI-000540 [Required: CSPR, PSPR] The product shall support the <service> element in the query which identifies the service for which this mapping is valid.

PSI-000560 [Required: CSPR, PSPR] The product shall support the <serviceNumber> element in the <mapping> response which contains the emergency services number appropriate for the location provided in the query. This allows a foreign end device to recognize a dialed emergency number.

PSI-000570 [Required: CSPR, PSPR] The PSPR shall support be configured to allow a requesting entity to obtain the boundary of the service area handled by the requested service, returned in the <serviceBoundary> element of <mapping>. This is most useful for mobile devices that use geodetic coordinates since they can track their location. When they leave the service area, they can send another <findService> request to determine the proper service area for their new location and avoid re-querying the PSPR provided they are within the returned boundary.

PSI-000580 [Required: CSPR, PSPR] The service boundary in a <mapping> shall support be returned by value and by reference. If the server returns a service boundary reference, the client shall then obtain the actual service boundary with a <getServiceBoundary> request.

Latitude/Longitude/Altitude

PSI-000590 [Required: GIS, LIS, SBC, PSPR] The LoST query shall support latitude and longitude to ensure geolocation accuracy. GML and geoshape elements require a srsName attribute to specify a URN that defines their interpretation. The system shall support latitude/longitude/altitude as the srsName attribute formatted as <gml:pos> with the latitude and longitude in decimal degrees.

3.1.4 IPV6

IP6-000011 [Required: All Products] - All products shall support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) stacks as described in RFC 8200. IPv6 shall also be implemented IAW USGv6 Capability Summary Strings (CSS) for each device type listed.

IP6-000050 [Required: All Products] - The system shall provide the same (or equivalent) functionality in IPv6 operation as it provides in IPv4 operation consistent with the requirements for the APL category.

IP6-000070 [Required: All Products] - The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 6085 and RFC 8064.

IP6-000100 [Conditional: All Products] - If Path MTU Discovery is used and a Packet Too Big message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU,

then the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet.

NOTE: Unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.

IP6-000150 [Required: All Products] - The product shall support the IPv6 Addressing Architecture as described in RFC 4291 and as updated by RFC 5952, RFC 6052, RFC 7136, RFC 7346, RFC 7371, and RFC 8064.

NOTE 1: According to DoD IPv6 Standard Profiles for IPv6-capable Products-Supplemental Guidance version 6.0, the use of IPv4-mapped addresses on the-wire is discouraged due to security risks raised by inherent ambiguities.

IP6-000160 [Required: All Products] - The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007 and updated by RFC 7346.

IP6-000180 [Conditional: All Products] - If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 environment, then it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 8415 and updated by RFC 4361, RFC 5494, RFC 6221, RFC 6422, RFC 6644, RFC 7083, RFC 7227, RFC 7283, RFC 7550.

IP6-000200 [Conditional: All Products] - If the product is a DHCPv6 client, then the product shall discard any messages that contain options that are not allowed to appear in the received message type (e.g., an Identity Association option in an Information-Request message).

IP6-000220 [Conditional: All Products] - If the product is a DHCPv6 client and the first retransmission timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, then the client shall continue with a client-initiated message exchange by sending a Request message.

IP6-000230 [Conditional: All Products] - If the product is a DHCPv6 client and the DHCPv6 solicitation message exchange fails, then it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs.

NOTE: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds.

IP6-000240 [Conditional: All Products] - If the product is a DHCPv6 client and it sends an Information-Request message, then it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.

IP6-000250 [Conditional: EI, NA/SS] - If the product is a DHCPv6 client, then it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server before transmitting packets using that address for itself.

IP6-000260 [Conditional: All Products] - If the product is a DHCPv6 client, then it shall log all reconfigure events.

NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).

IP6-000270 [Conditional: All Products] - If the product supports DHCPv6 and uses authentication, then it shall discard unauthenticated DHCPv6 messages from DOD Information Network (DODIN) Products and log the event.

NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).

IP6-000280 [Required: All Products] - The product shall support Neighbor Discovery for IPv6 as described in RFC 4861 and updated by RFC 5942, RFC 6980, RFC 7048, RFC 7527, RFC 7559, RFC 8028, RFC 8319, RFC 8425 as appropriate to their role as an IPv6 End Node or IPv6 Intermediate Node. Informational RFC 4943 provides additional background on implementation of Neighbor Discovery (ND). Note: ND implies that nodes MUST support Multicast Listener Discovery.

IP6-000430 [Required: All Products] - If the product supports IPv6 SLAAC, then the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product shall have a configurable parameter that allows the managed address configuration flag and the other stateful configuration flag to always be set and not perform stateless auto configuration.

IP6-000450 [Required: All Products] - While nodes are not required to auto configure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862 as updated by RFC 7527. In accordance with RFC 4862 as updated by RFC 7527, DAD shall be implemented and shall be on by default.

IP6-000460 [Required: All Products] - A node shall allow for auto configuration-related variable to be configured by system management for each multicast-capable interface to include DupAddrDetectTransmits where a value of zero indicates that DAD is not performed on tentative addresses as specified in RFC 4862 as updated by RFC 7527.

NOTE: Network Infrastructure Security Technical Implementation Guide (STIG) states the following: The use of Duplicate Address Detection opens the possibility of denial-of-service attacks. Any node can respond to Neighbor Solicitations for a tentative address, causing the other node to reject the address as a duplicate. This attack is like other attacks involving the spoofing of Neighbor Discovery messages. Further, RFC 4862 as updated by RFC 7527 states the following: By default, all addresses should be tested for uniqueness prior to their assignment to an interface for safety. The test should individually be performed on all addresses obtained manually, via stateless address auto configuration, or via DHCPv6. To accommodate sites that believe the overhead of performing Duplicate Address Detection outweighs its benefits, the use of Duplicate Address Detection can be disabled through the administrative setting of a per-interface configuration flag. The products may include an administrative setting to disable DAD.

IP6-000470 [Required: All Products] - The product shall support manual assignment of IPv6 addresses.

IP6-000520 [Required: All Products] - The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443 and updated by RFC 4884.

IP6-000550 [Conditional: All Products] - If the product has the capability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address, the product shall support the disabling of this capability.

NOTE: The number of responses may be traffic conditioned to limit the effect of a denial-of-service attack.

IP6-000740 [Conditional: All Products] - If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.

IP6-000890 [Conditional: All Products] - If IPv6-compatible nodes are managed via Simple Network Management Protocol (SNMP) using IPv6, then the product shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293 which obsoletes RFC 2011, RFC 2465, and RFC 2466.

IP6-000900 [Conditional: All Products] - If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support the SNMPv3 management framework as described in RFC 3411 which obsoletes RFC 2571, and is updated by RFC 5343, RFC 5590.

IP6-000910 [Conditional: All Products] - If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support SNMPv3 message processing and dispatching as described in RFC 3412 which obsoletes RFC 2572, and is updated by RFC 5590.

IP6-000920 [Conditional: All Products] - If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support the SNMPv3 applications as described in RFC 3413 part of STD 62 which obsoletes RFC 2573.

IP6-000930 [Conditional: All Products] - If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the IP MIBs as defined in RFC 4293 which obsoletes RFC 2011, RFC 2465, and RFC 2466.

IP6-000940 [Conditional: All Products] - If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022.

IP6-000950 [Conditional: All Products] - If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the User Datagram Protocol (UDP) MIBs as defined in RFC 4113.

IP6-000970 [Conditional: All Products] - If the product performs routing functions and is managed by SNMP using IPv6, then the product shall support the IP Forwarding MIB as defined in RFC 4292.

IP6-001000 [Conditional: All Products] - If the product uses the Domain Name Service (DNS) resolver for IPv6 based queries, then the product shall conform to RFC 3596 a.k.a. STD 88 for DNS queries.

IP6-001040 [Required: All Products] - The product shall forward packets using the same IP version as the version in the received packet.

NOTE: If the packet was received as an IPv6 packet, then the appliance shall forward it as an IPv6 packet. If the packet was received as an IPv4 packet, then the appliance shall forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur.

IP6-001120 [Required: SBC] - The product shall be able to provide topology hiding [e.g., Network Address Translation (NAT)] - for IPv6 packets as described in Cybersecurity Section.

NOTE: Deployments requiring the network topology hiding that IPv4 NAT provided as a side-effect should consider RFC 4864 – Local Network Protection (LNP) for IPv6.

AUX-003880 [Required: All Products] - The system or network device shall be able to set DSCPs on both signaling packets and media streams for both IPv4 and IPv6 as specified in the Traffic Conditioning Specification Section.

CYB-061000 [Required: All Products] - The product shall support the capability to verify that the identity claimed in an X.509v3 certificate Subject Common Name, used to establish an authenticated and secure channel, correctly maps to the identity claimed in signaling messages transmitted within the same secure channel.

NOTE1: At this time the identity claimed in an X.509v3 certificate Subject Common Name may be a FQDN, IPv4, or IPv6 address.

NOTE2: The Subject Common Name is expected to *map* to the identity claimed in signaling messages, but this mapping does not mean that the Subject Common Name and the identity in the signaling messages are identical or related. For example, the identity claimed in a signaling message may be 1234567890@uc.mil, and this might be compared to a CAC Subject Common Name of Doe. John. A. 2378324324 to verify that the certificate presented in the CAC maps to the claimed phone number for authorization purposes.

CYB-061010 [All Products] - The product shall support the capability to examine the identity claimed by the X.509v3 Subject Common Name field and compare it to the identity claimed within signaling messages regardless of whether the claimed identity contains an FQDN, IPv4 address, or IPv6 address.

3.1.5 SIP

SIP-000010 [Required: All Products] All SIP devices must support SIP in accordance with RFC 3261 and offer-answer in accordance with RFC 3264.

SIP-000020 [Required: All Products] SIP devices must implement TCP.

SIP-000030 [Required: All Products] All SIP devices must support TLS which includes DOD Public Key Information (PKI) and Federal Information Processing Standards (FIPS) 140-2 or 140-3 validated modules.

SIP-000040 [Required: All Products] All SIP devices must support TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_RSA_WITH_AES_128_CBC_SHA.

SIP-000050 [Required: All Products] All SIP devices shall support TLS (dual path method) to provide confidentiality for the SIP messages as described in RFC 3261.

SIP-000060 [Required: All Products] All SIP devices shall support Online Certification Status Protocol (OCSP).

SIP-000070 [Required: All Products] The system must support voice samples received from SIP end instruments using the real-time transport protocol (RTP) as described in RFC 3550 and

MUST support SRTP RFC 3711 using SDP security descriptions RFC 4568 for the necessary key exchange.

SIP-000080 [Required: All Products] The system must support MUST use the confidentiality mechanisms in SRTP and SRTCP and support Symmetric RTP/SRTP to ensure media confidentiality as described in [RFC 3711].

SIP-000090 [Required: All Products] The SRTP media port range must be configurable between 2048 and 65535 with the default between: 16384 to 32764.

SIP-000100 [Required: All Products] The system must support PRACK, 100rel option tag in accordance with RFC 3262.

SIP-000110 [Required: All Products] The system MUST support the following CODECs: G.711 μ-Law, G.711 a-Law, Dual Tone Multi-Frequency (DTMF) via RFC 4733, G.729 or G.729A, T.38, RFC 4040 64 Kbps Clearmode, V.150.1 Modem Relay (Media Gateways /vIPers), NoAudio (SCIP-215, For Secure Communications Interoperability Protocol (SCIP) secure only phones).

SIP-000120 [Required: All Products] The system must support Session Controllers sending changes to negotiated media capabilities via SIP. SIP re-INVITE MUST support [RFC 3261], Section 14 of the SIPconnect 2.0 Technical Recommendation "Modifying an Existing Session." SIP UPDATE MUST be used for this purpose when both endpoints advertise support for [RFC 3311].

The following SIP requirements from UCR 2013, Change 2 are required:

SIP-009581 [Required: All Products] SIP signaling appliances MUST support generating and receiving the SUBSCRIBE method for event notification (RFC 3265).

SIP-009591 [Required: All Products] SIP signaling appliances MUST support the NOTIFY method for event notification defined in RFC 3265. This specification uses the NOTIFY request in the call transfer supplementary service.

3.1.5.1 Emergency Services

SIP-000130 [Required: SC, SBC, CSPR] The system MUST be able to recognize emergency calls (i.e., 9-1-1) and route that call to the CSPR. It MUST populate the Request-URI using a dial string Uniform Resource Identifier (URI), in accordance with NENA-STA-010.3d-2021 that contains the national emergency services number.

SIP-000140 [Required: All Products] The system MUST recognize the identity of the caller in the "P-Asserted-Identity" header field, in accordance with the rules of RFC 3325 and RFC 5876, and in the "From" header field URI with a URI that the Session Controller wishes to be used for caller identification.

SIP-000150 [Required: All Products] The system MUST NOT withhold the "P-Asserted-Identity" header field for privacy reasons and MUST NOT anonymize the "From" header field. All products shall pass the INVITE with identity of the caller in the "P-Asserted-Identity" header field, in accordance with the rules of RFC 3325 and RFC 5876, and in the "From" header field URI with a URI that the SC wishes to be used for caller identification.

SIP-010160 [Required: All Products] The SC shall not withhold the "P-Asserted-Identity" header field for privacy reasons and shall not anonymize the "From" header field. Products in the call path shall not anonymize the "From" header field.

SIP-010165 [Required: CSPR] The CSPR shall be able to recognize emergency calls based on the presence of the agreed emergency services number in the Request-URI.

SIP-000170 [Required: All Products] If an originating session is an emergency session, then SIP session limits do not apply. The CSPR shall NOT apply SIP session limits to emergency calls originated by a Session Controller. The Session Controller and the SBC shall NOT apply SIP session limits to emergency services calls.

SIP-000180 [Required: All Products] Information relating to the location of a SC user or EI shall be provided depending on local regulatory requirements. The SC or EI when providing location SHALL support do so using the SIP Geolocation Header field as specified in RFC 6442, location MAY be provided by value or by reference.

3.2 System Availability

SCM-001861 [Ref UCR: SCM-001860] **[Required: CSPR, SBC, SC]**

Call survivability: connect first time and call remains active until either the call originator or terminating end disconnects.

a) No Loss of Active Sessions. In the event of component failure in an appliance subsystem(s), all active sessions shall not be disrupted (namely, the loss of established session connections requiring user redialing to reestablish), and the media path through the network shall be restored within 5 seconds. In addition, when the state information is lost for non-disrupted active sessions, the Secure Real-time Transport Protocol (SRTP) media streams will clear when both the called and calling parties hang up their End Instrument (EIs).
b) Software Upgrades and Patches. Software upgrades and patches shall be able to be implemented without incurring any subsystem downtime.
c) System must support a minimum Mean Opinion Score (MOS) score of 4.0 or better for SIP calls.

4 FUNCTIONAL ELEMENT REQUIREMENTS

4.1 CSPR

The CSPR is the DoD product category for the NENA i3 ESRP functional element. The functionality of the ESRP comprises the NENA i3 Policy Routing Function (PRF).

Typically, an emergency services call is received via an SBC to the CSPR, the CSPR shall query the PSPR and refer the call to the servicing PSAP/ECC. It is possible the CSPR may tandem the call to an intermediary CSPR before delivering to the destination PSAP/ECC. The destination of the call on the output of the CSPR is conceptually a queue, represented by a URI. In most cases, the queue is maintained on a downstream CSPR, and is most often empty. However, when the network gets busy it is possible for another PSAP/ECC to receive calls from the queue. The queue is most often First-In First-Out, but in some cases, there can be out-of-order selections from the queue.

Policy-based routing is a networking technique that allows administrators to create and enforce specific rules for routing traffic within a network. This can be useful in a variety of situations, such as prioritizing certain types of traffic, directing traffic to specific devices or networks, or implementing security measures.

Policy-based routing provides the ability to customize routing decisions based on a variety of factors, such as the source and destination of traffic, the type of traffic being transmitted, and the status of network devices. This facilitates call routing decisions based on real time call progression data based on, but not limited to Secure Telephone Identity Revisited (STIR) /Signature-based Handling Information Using toKENs (SHAKEN) attestation level, network call abuse patterns, and/or PSInet call load metrics.

The CSPR processes administrative calls using the policy routing function inherent in the CSPR to leverage policy-based routing. Emergency services calls trigger the CSPR to query the PSPR for location validation and route determination the CSPR uses this additional location information to make the final policy-based routing decision.

4.1.1 CSPR Interface Support Requirements

The CSPR requirements are located the DISA Soft Switch Backbone SRD.

4.2 PSPR

4.2.1 Summary

Emergency calls shall be routed to the appropriate PSAP/ECC based on the location of the caller. In addition, PSAP/ECCs may utilize the same routing functionality to determine how to route emergency calls to the correct responder. The NG9-1-1 functional element responsible for providing routing information to the various querying entities is the PSPR. A PSPR provided by DISA and accessible from the PSInet shall permit querying by an IP client/endpoint, an IP routing proxy belonging to, a CSPR in a next generation Public Safety network, or by some combination of these. DISA shall provide a PSPR to replicate Forest Guide (FG) functionality as part of the MPG as required.

The DOD shall consolidate the NENA i3 defined functional elements ECRF, LVF, and FG into the PSPR product category due to the overlap of functionality. The ECRF and LVF functions

have the same interfaces and contain the same data. They may be combined into a single implementation. However, it should be noted that the ECRF is a real-time element in the signaling path of an emergency call.

4.2.2 Standards

PSP-000010 [Required: PSPR] PSPR shall comply with NENA-STA-010.3b-2021 Sec 4.3

PSPR shall comply with NENA-STA-010.3b-2021 Sec 4.13

PSP-000020 [Required: PSPR] The system shall comply with NENA-STA-005.1.2-2022.

4.2.3 Set of requirements

PSP-000030 [Required: PSPR] A PSPR accessible inside the PSInet shall permit querying from any Emergency Service entity inside the PSInet.

PSP-000040 [Required: PSPR] The PSPR shall route SIP calls based off an FQDN and the SIP URI therefore all elements identified by hostnames SHALL have corresponding Domain Name Service (DNS) records as specified in STD13 (RFC 1034) in the DOD DNS.

PSP-000050 [Required: All Products] All elements connected to the PSInet shall support a local DNS resolver to translate hostnames they receive to IP addresses.

PSP-000060 [Conditional: PSPR] When a caching DNS resolver in the PSInet cannot refresh an expired cached resource record in response to a query because the authoritative DNS server is not available, it should reuse the stale cached resource record as though the cached resource record's TTL is 1 second, as described in Section 4 of RFC 8767.

PSP-000070 [Required: PSPR] DNSSEC (RFC 4035) SHALL be deployed in authoritative DNS servers, especially those resolving names found in external PSPRs.

PSP-000080 [Required: PSPR] A domain that has SIP elements within the domain SHALL have an SRV record RFC 2782 for a SIP service for the domain, and any of its subdomains that may appear in a URI.

PSP-000090 [Required: CSPR, PSPR] Placing a LoST query always requires resolution of an Application-Unique String (AUS), which is in the form of an FQDN via U-NAPTR (RFC 4848), and U-NAPTR resolution may also be required to obtain the URI for a LIS (per RFC 5986)

Route Query

PSP-000100 [Required: PSPR] When an PSPR receives a LoST query (as defined in IETF RFC 5222), it determines whether the query was received from an authenticated entity (e.g., an CSPR) and the type of service requested (i.e., emergency services).

PSP-000110 [Required: PSPR] Authentication shall apply to all entities that initiate queries to the PSPR within the PSInet. TLS is used by all PSPRs within the PSInet, and credentials issued to the querying entity that are traceable to a DOD Certificate Authority (CA) shall be accepted.

PSP-000120 [Required: PSPR] Devices and carriers outside the PSInet may not have DoD credentials, therefore the PSPR should assume a common public identity for such queries. Based

on the service requested, the PSPR determines which URI is returned in the LoST response. This URI may be a SIP Point-of-Interconnect to the PSInet, a URI of a PSAP/ECC, or another CSPR. This is applicable to the MPG interconnection to external ESInets.

PSP-000130 [Required: PSPR] The PSPR is provisioned with a service boundary layer containing one or more service boundary polygons. Each of the polygons shall have attributes that specify the service URN that the polygon applies to and the mapping the PSPR should return if the provided location is within the polygon.

PSP-000140 [Required: PSPR] The PSPR shall return the URI attribute of the service boundary matching the URN that contains the location from PSP-000130.

PSP-000150 [Conditional: PSPR] The querier shall have local policy to determine how to handle potential conflicts in returned data. In some cases, the PSPR may use the identity of the querier, or a distinguished service URN to return the URI of the correct agency. This condition only occurs for queries to an PSPR from within a PSInet.

Note: External queries shall only return one URI. If the proffered location is not specified as a point (that is the location in the query is a shape) and the shape intersects more than one service boundary with a given service URN, the PSPR response should be the URI of the service boundary with the greatest area of overlap (with a tie breaking policy for the case of equal area of overlap). If more than one service boundary for the same service URN at a given location (point or civic address) exists in the CSPR, multiple elements are returned.

Service Boundary

PSP-000160 [Required: PSPR] Location shall be represented by geodetic coordinates providing data that corresponds to a specific geographic location shape. A service boundary is represented by a polygon set. More than one polygon may occur in the set, for example, when the service area has holes or non-contiguous regions.

PSP-000170 [Required: PSPR] For each service URN supported by an PSPR, one or more layers shall provide polygon sets associated with URIs. Two types of attributes are associated with these polygons:

- URN: the service URN this boundary is associated with.
- URI: a URI returned if the location is within the boundary.

PSP-000180 [Required: PSPR] The PSPR shall compute a response to a LoST query by finding the polygon with the service URN attribute matching that the one provided in the LoST query containing the location and returning the URI attribute of that polygon set. If the proffered location is a shape, that shape may overlap more than one service boundary. The response in that case may be determined by an algorithm in the PSPR and should be the greatest area of overlap but is not otherwise specified in the present document.

PSP-000190 [Required: PSPR] Emergency service authorities shall be responsible for the authoritative data for their jurisdiction in the PSPR. The data may be aggregated at a regional, MILDEP, or global, and the PSPR system provided at that level may be the responsibility of the associated emergency communications agency.

PSP-000200 [Conditional: PSPR] Originating network operators may maintain replicas of the PSPR. Thus, the operation and maintenance of individual PSPRs may be the responsibility of the

provider of the network in which they physically reside, but it is the emergency service authority that is responsible for maintaining the integrity of the source data housed within those systems. The authority may also provide input to the definition of the policy which dictates the granularity of the routing data returned by the PSPR (i.e., CSPR URIs vs. PSAP URIs), based on the identity of the query originator and/or service URN.

Location Validation

PSP-000210 [Conditional: PSPR] When the PSPR is responding as a location validation service where civic location information is validated against the authoritative GIS database information. A civic address shall be considered valid if it can be located within the database uniquely, is suitable to provide an accurate route for an emergency call, and adequate and specific enough to direct responders to the right location.

PSP-000220 [Required: PSPR] PSPR shall support a PSAP/ECC query to validate locations not received through incoming call signaling.

PSP-000230 [Required: PSPR] The PSPR shall support LoST as specified RFC 5222

4.3 Location Information Server (LIS)

4.3.1 Summary

LIS (Location Information Server) is a functional element that provides locations of endpoints. The LIS is not part of the NGCS, but rather NG9-1-1 required equipment provided and maintained within the mission-partner voice enclave. *The LIS functionality may be included in the Telephony Management System* based on this overlapping functionality. A LIS can provide Location-by-Reference, or Location-by-Value, and, if the latter, in geodetic or civic forms. A LIS can be queried by an endpoint for its own location, or by another entity for the location of an endpoint. In either case, the LIS receives a unique identifier that represents the endpoint, for example an IP address, circuit-ID, or Media Access Control (MAC) address, and returns the location (value or reference) associated with that identifier. The LIS is also the entity that provides the dereferencing service, exchanging a location reference for a location value.

Location is fundamental to the operation of the emergency services, and the generic functional entity that provides location is a Location Information Server (LIS). For the purposes of the present document, the only capabilities a LIS provides that are relevant are:

1. A dereference function defined for location by reference
2. A function defined for location requests including different identities
3. A function to permit requests from third parties

4.3.2 Set of requirements

LIS-000010 [Required: LIS] The LIS shall accept a HELD request for location as defined in section **Error! Reference source not found.** of this document.

LIS-000020 [Required: LIS] The LIS shall respond to a querier with a HELD response as defined in **Error! Reference source not found.** and provide a PIDF-LO response as defined i n section 0.

LIS-000030 [Required: LIS] The LIS shall provide a mechanism to populate the location database via one or more of the following methods: manual input, DHCP via options, or access switch discovery via SNMP.

LIS-000040 [Required: LIS] The LIS shall query a GIS repository based on the structure in NENA-STA-006.2-2022

LIS-000050 [Required: LIS] The system shall be consistent with the most current NENA i3 standard (NENA STA-010.). The system shall implement both SIP Presence Event Package and HELD dereferencing interfaces to any LIS function as described in NENA i3 standard Section 4.10.

LIS-000060 [Required: LIS] The LIS may support SIP Presence to provide location-by-reference as defined by IETF RFC 5808. Using SIP Presence, the entity desiring location subscribes to the SIP Presence Event Package (IETF RFC 3856) at the location URI provided. The LIS sends NOTIFY transactions (IETF RFC 6665) containing a PIDF document that shall include the location in the Location Object (LO) part, forming the PIDF-LO.

LIS-000070 [Required: LIS] An immediate NOTIFY shall be generated by the LIS upon acceptance of a subscription request. This would represent the current location of the target. The SUBSCRIBE includes an Expires header (IETF RFC 3261) which represents the subscribers requested expiration, and the 2XX response contains one that represents the server's actual expiration (which may be shorter, but not longer, than the subscriber's requested time).

LIS-000080 [Required: LIS] The LIS shall support an Expires header with a value of zero indicating a request for exactly one NOTIFY (that is the current location) with no further updates. Subscriptions expire when the call terminates if the LIS is call-aware.

LIS-000090 [Required: LIS] The LIS shall support rate limits (IETF RFC 6446) and Location filters (IETF RFC 6447) and shall be supported by the LIS if it supplies a SIP location URI. The querier shall limit how often further NOTIFYs are sent (before expiration of the subscription) using a filter (IETF RFC 4661).

LIS-000100 [Required: LIS] When location is provided by reference the reference shall be valid, at least for the length of the call.

LIS-000110 [Conditional: LIS] If the LIS supplies location by reference, it shall provide a dereferencing service for that location URI it supplies: given the URI, the LIS provides the location value as a PIDF-LO. A LIS may be a database, or a protocol interworking function to an access network specific protocol, or both. As a Location Server (LS), the LIS shall explicitly authorize requests from third parties (refer to IETF RFC 6155, section 4.2.). Elements in the PSInet, including the PSPR and PSAP/ECC may dereference a location URI as part of processing a call.

Note: The operation use of location by reference may be problematic within DoD networks due to the crossing of multiple security boundaries. The likely outcome is the LIS will not be reachable by the PSPR or PSAP/ECC for dereferencing.

LIS-000120 [Required: LIS] A Location Information Server shall supply location in the form of a PIDF-LO (location by value) and a location URI (location by reference) as in section 3.1.1.1 of this SRD.

LIS-000120 [Required: LIS] The LIS shall supply location (by value or reference) to the endpoint, or proxy operating on behalf of the endpoint. The resulting PIDF-LO or location URI shall appear in the initial SIP message in a Geolocation header.

LIS-000120 [Optional: LIS] The LIS may support SIP Presence to provide location-by-reference as defined by IETF RFC 5808. Using SIP Presence, the entity desiring location subscribes to the SIP Presence Event Package (IETF RFC 3856) at the location URI provided. The LIS sends NOTIFY transactions (IETF RFC 6665) containing a PIDF document that shall include the location in the Location Object (LO) part, forming the PIDF-LO.

4.4 SI/GIS

4.4.1 GIS Datastore Summary

The GIS datastore is a central, authoritative repository for location data for the PSInet. The GIS datastore is an aggregate database feed from child/local databases. The GIS datastore contains data all the locations serviced by the PSInet.

4.4.2 Set of requirements

GIS Data Model which supports the NENA NGCS of location validation and routing, both geospatial call routing to the appropriate location for dispatch. This model also defines several GIS data layers (layers) used in local PSAP/ECC and response agency mapping applications for handling and responding to 9-1-1 calls.

GIS-000010 [Required: GIS] The GIS datastore shall accept validated data from data owners (child databases).

GIS-000020 [Required: GIS] The GIS datastore shall identify data discrepancies and shall provide a mechanism to communicate discrepancies to data owners in accordance with NENA-STA-010.3d-2021 sec. 3.7.

GIS-000030 [Required: GIS] The GIS datastore shall conform to the GIS data and database structure of NENA-STA-006.2-2022.

GIS-000040 [Required: GIS] The GIS datastore shall provide a mechanism to set policies based on data discrepancy.

GIS-000050 [Required: GIS] The GIS datastore shall support Open Geospatial Consortium (OGC) Webservices interface to the Spatial Interface (SI).

GIS-000060 [Optional: GIS] The GIS datastore may support a file transfer or other interface to the Spatial Interface (SI).

4.4.3 SI Summary

The SI contains the database elements applicable to the PSInet routing and the interfaces required to synchronize that data to LIS and PSPR elements.

4.4.4 Set of requirements

GIS-000070 [Required: GIS] The data model employed in support of the location services configuration shall be delivered in accordance with NENA-STA-006.2-2022.

GIS-000080 [Required: GIS] The system employed shall support the provisioning and maintenance of GIS data to PSPR in accordance with NENA-STA-005.1.2-2022.

GIS-000090 [Required: GIS] LIS and PSPR elements shall be able to query this service for relevant GIS data.

GIS-000080 [Required: GIS] The SI shall support an OGC Web Feature Service (WFS) interface for data interchange with LIS, PSPR elements.

4.5 PSAP/ECC

A PSAP/ECC is a service, typically composed of more than one functional element. The functional elements that make up a PSAP/ECC are defined in NENA STA-023.1-2021. PSAP/ECC Specifications for the NENA i3 Solution (forthcoming). A PSAP/ECC provides the following interfaces towards the PSInet.

4.5.1 SIP Call interface

PCH-000010 [Required: PSAP Call Handling] The PSAP/ECC SHALL deploy the SIP call interface that complies with SIPconnect including the multimedia capability, and non-interactive call (emergency event) capability.

PCH-000020 [Required: PSAP Call Handling] PSAP/ECC SHALL recognize calls to their administrative numbers received from the PSInet (and distinguishable from normal 9-1-1 calls by the presence of the number in a sip or tel URI in the To header field and the absence of the sos service URN in a Request-URI line.

PCH-000030 [Optional: PSAP Call Handling] The SIP call interface MAY also be used to place non 9-1-1 calls (including callbacks) from the PSAP/ECC.

PCH-000040 [Required: PSAP Call Handling] Callback and other non-emergency outbound call INVITE messages SHALL comply with the SIPconnect call interface, and constructed using the guidance provided in section 4.20 of NENA -STA-010.3d-2021, with the following clarifications:

- The To header field value of the callback INVITE message SHALL be set to a value that allows reaching the home network of the target. If the To header field

value is a tel URI, the OCIF shall route the callback toward the PSTN, which means that only the voice portion shall go through. If the To header field value is a sip URI, the domain SHALL be the one of the home network of the target. The Request-URI line SHOULD contain the same URI value as in the To header field.

PCH-000050 [Required: PSAP Call Handling] PSAP/ECC SHALL support all media, voice, video, and text.

PCH-000060 [Required: PSAP Call Handling] If a PSAP/ECC receives an Offer containing both MSRP and RTT, it SHALL send an Answer with only one of them.

PCH-000070 [Required: PSAP Call Handling] If the PSAP/ECC receives an Answer containing both RTT and MSRP, it SHALL be prepared to deal with both simultaneously.

PCH-000080 [Required: PSAP Call Handling] In the event a caller is disconnected from a PSAP/ECC the PSAP/ECC call handling system shall have a capability to call back the caller.

PCH-000090 [Required: PSAP Call Handling] When placing callbacks, PSAP/ECCs SHALL offer all supported media choices, subject to operational considerations.

PCH-000100 [Required: PSAP Call Handling] Emergency calls marked with a humintlang tag (RFC 8373) SHALL be processed with appropriate language-specific resources available to the PSAP/ECC .

PCH-000110 [Required: PSAP Call Handling] SDP offers and answers generated by the PSAP/ECC SHALL include appropriate language tags.

PCH-000120 [Required: PSAP Call Handling] Answers to offers that included language tags SHALL include language tags; however, the PSAP/ECC is not obligated to offer languages it supports with outside entities such as a language translation service.

PCH-000130 [Required: PSAP Call Handling] The PSAP/ECC shall support LoST as defined in section 3.4 of NENA-STA-010.3d-2021.

PCH-000140 [Required: PSAP Call Handling] The PSAP/ECC shall support LoST to query the PSPR to handle calls that shall be dispatched and calls that shall be transferred based on the actual location of the incident.

PCH-000150 [Required: PSAP Call Handling] The LoST interface shall use the “urn:emergency:service:responder” URNs to achieve “selective transfer” operations.

PCH-000160 [Optional: PSAP Call Handling] The PSAP/ECC MAY also use the LoST interface to find an AgencyLocator URI by location by querying the PSPR with a service URN of a subservice of “urn:emergency:service:serviceagencylocator”. The AgencyLocator record can be retrieved from the URI by dereferencing it with HTTPS GET.

PCH-000170 [Required: PSAP Call Handling] The PSAP/ECC shall support HELD.

PCH-000180 [Required: PSAP Call Handling] The PSAP/ECC shall implement both SIP Presence Event Package and HELD dereferencing interfaces to any LIS function.

PCH-000190 [Required: PSAP Call Handling] The PSAP/ECC shall support TCP with TLS for the LIS dereferencing interface.

4.5.2 Test Calls

PCH-000200 [Required: PSAP Call Handling] PSAP/ECCs SHALL support the test call interface as described in Section 9 of of NENA STA-023.1-2021

PCH-000210 [Required: PSAP Call Handling] The PSAP/ECC shall support the following send call request schema identified by the PSAP ID:

HTTP method: PUT

Resource name .../ SendCallRequests/{psapId}:

Parameters:

Name	Condition	Description
psapId	Required	AgencyId of the PSAP that wishes to have test calls sent to it
location	Required	PIDF-LO used for location of test calls
frequency	Required	Minutes between test call send
discrepancyRateLimit	Required	Max number of Discrepancy Reports per hour
startDate	Required	When to start sending test calls
endDate	Required	When to stop sending test calls
testConditions	Required	PrrTest conditions (see below) for the test

PCH-000220 [Required: PSAP Call Handling] The PSAP/ECC shall support the following status codes:

- 200 OK
- 442 Unacceptable Parameters
- 454 Unspecified Error
- 458 Policy Violation

4.5.3 Call Diversion

PCH-000230 [Required: PSAP Call Handling] A PSAP/ECC may become overloaded and be unable to answer every call. Overload is determined by exceeding the size of the primary queue to which its calls are sent.

PCH-000240 [Required: PSAP Call Handling] Routing rules for shall support the following alternate call treatments:

- Calls sent a “Busy” indication;
- Calls diverted to an Interactive Media Response unit;
- Calls diverted to one or more alternate PSAP/ECCs.

4.5.4 Bridge Interface

PCH-000230 [Required: PSAP Call Handling] The PSAP/ECC shall deploy a bridge inside the PSAP, it shall provide the bridge controller interfaces.

PCH-000240 [Required: PSAP Call Handling] PSAP/ECCs shall be able to accept calls from, and utilize the features of, outside bridges.

PCH-000250 [Required: PSAP Call Handling] The interface shall support the functionality in Section 4.7 of NENA STA-023.1-2021.

4.5.5 Computer Aided Dispatch (CAD) / Unified CAD (UCAD)

CAD systems are utilized by dispatchers, call-takers, and 911 operators to prioritize and record incident calls, identify the status and location of responders in the field, and effectively dispatch responder personnel. Emergency responders in the field can receive messages initiated by CAD systems via their mobile data terminals (MDTs), radios, and cell phones. CAD systems may also interface with a GIS, an automatic vehicle location (AVL) system, a caller identification (ID) system, logging recorders, and various databases. A UCAD system interfaces with multiple agencies and/or computer systems that serve law enforcement, fire, and EMS and provides communication across multiple agencies and jurisdictions.

CAD-000010 [Required: PSAP CAD] When a dispatcher receives a call, the CAD system shall display the location of the caller.

CAD-000020 [Required: PSAP CAD] The CAD system shall allow the dispatcher to log additional information relevant to the incident.

CAD-000030 [Required: PSAP CAD] Logging recorders can store information such as call time and duration for later retrieval.

CAD-000040 [Required: PSAP CAD] The CAD system shall provide the following to the dispatch center:

- Log on/log off times of emergency personnel;
- Time stamping of all communications;
- Case numbers for investigations;
- Assignments of emergency personnel; and
- Incident reports and archives.

CAD-000050 [Required: PSAP CAD] The CAD systems shall meet the minimum requirements documented in Association of Public Safety Communications Officers (APCO) document ANS 1.110.1-2015 Multi-Functional Multi-Discipline CAD Minimum Functional Requirements.

Note: The Multi-Functional Multi-Discipline CAD Minimum Functional Requirements standard identifies the minimum functional requirements that a CAD system shall include, broken down by public safety discipline. Also identified are the optional functional requirements that a CAD system should include.

CAD-000060 [Required: PSAP CAD] CAD interoperability between DoD CAD information systems, and with NG9-1-1 call handling systems shall employ the Emergency Incident Data Object (EIDO). This shall be based on the JavaScript Object Notation (JSON) object that contains incident and related information intended to be passed between functional elements comprising the NG9-1-1 ecosystem.

Note: Most interactions between FEs inside a PSAP/ECC, between PSAP/ECCs, and between PSAP/ECCs and other entities, involve sending and receiving an EIDO.

CAD-000070 [Required: PSAP CAD] All transmissions of EIDOs shall use TLS security employing NIST FIPS 140-3 encryption hashes. Any existing CAD systems currently certified to operate using FIPS 140-2 can continue to operate until their ATO has to be renewed, at which time the product shall support FIPS 140-3 certified algorithms.

CAD-000080 [Required: PSAP CAD] The content of an EIDO shall conform to the data rights management policy of the owner of the data per the DoD policy.

CAD-000090 [Required: PSAP CAD] all implementations shall accept EIDOs of any size up to and including 10,485,760 bytes (ten megabytes).

4.5.6 Logging Service

CAD-000100 [Required: PSAP CAD] The PSAP/ECC shall implement a Logging Service client, as defined in Section 4.12 of NENA STA-023.1-2021, including the client side of the media recording mechanism (Section 4.12.2 of NENA STA-023.1-2021).

CAD-000110 [Optional: PSAP CAD] The PSAP/ECC MAY deploy a Logging Service (as described in Section 4.12 of NENA STA-023.1-2021) inside the PSAP/ECC, in which case it shall provide the Logging Service retrieval functions.

CAD-000120 [Conditional: PSAP CAD] A PSAP/ECC shall be able to use a Logging Service hosted in the PSInet.

4.5.7 Time Interface

CAD-000130 [Required: PSAP CAD] The PSAP/ECC shall implement an NTP client interface for time-of-day information. The PSAP/ECC may also provide an interface to a hardware clock.

4.5.8 GIS

CAD-000140 [Required: PSAP CAD] The PSAP/ECC shall support an OGC Web Mapping Service (WMS) interface.

CAD-000150 [Required: PSAP CAD] The PSAP/ECC shall provide a GIS server interface, as described in Section 3.6 of the NENA-STA-010.3d-2021, for the PSPR, GIS SI, and other interfaces.

CAD-000160 [Conditional: PSAP CAD] The PSAP/ECC should provide the MSAG Conversion Service (server side) or may use an PSInet service (client side).

REQUIREMENTS

4.6 SBC

The SBC shall support the requirement in the Soft Switch Backbone SRD and UCR 2013, Change 2 with the following additions or changes.

4.6.1 SBC Requirements

SBC-00040 [Required: SBC] the SBC shall support SIP in accordance with IETF RFC 6261. This requirement replaces the need for the SBC to support Assured Service SIP (AS-SIP) as defined in UCR 2013, Change 2.

SBC-00050 [Required: SBC] the SBC shall support HELD (RFC 6155) in order to process emergency service calls. The SBC shall support a SIP header with an XML schema (Presence Information Data Format – Location Object (PIDF-LO).)

SBC-00060 [Required: SBC] The SBC shall include the functionality of the Border Control Function (BCF) as defined in the NENA i3 specification.

SBC-000070 [**Required: SBC**] [Ref UCR: SCM-005660] To enable full topology hiding [Network Address Translation (NAT)] of signaling and bearer traffic, the enclave-fronting SBC shall function as the outbound and inbound signaling proxy for all SIP signaling traffic exchanged between AEIs and the centralized ESC.

SBC-000080 [**Required: SBC**] [Ref UCR: SCM-005670] For the routing of SIP signaling traffic exchanged between AEIs and the centralized ESC, the enclave-fronting SBC shall be capable of maintaining a persistent TLS connection with every served AEI within the enclave and the ESC-fronting SBC. NOTE: In an ESC Cluster configuration, the ESC cluster member may reside within the local enclave (e.g., in the case of an Environment 1 or 2 site). In this particular use case, the served AEIs within the enclave shall maintain a persistent TLS connection with the local cluster member.

SBC-000090 [Required] [Ref UCR: SCM-005680] The enclave-fronting SBC shall function as a registration proxy for all EIs located within the associated enclave:

a. When a served EI sends an SIP REGISTER request to the enclave-fronting SBC, the enclave-fronting SBC shall replace the IP address and port value contained in the Contact header of the REGISTER message (i.e., the inside-address/port) with an IP address and port value associated with a WAN-facing interface on the enclave-fronting SBC (i.e., the outside-address/port). NOTE: In an ESC Cluster configuration, the ESC cluster member may reside within the local enclave (e.g., in the case of an Environment 1 or 2 site). In this particular use case, the served EIs within the enclave shall send their SIP REGISTER request to the local cluster member.

b. For the life of the registration, the enclave-fronting SBC shall maintain a binding between the inside-address/port and outside-address/port.

c. When the enclave-fronting SBC receives an inbound SIP request/response where the embedded address (e.g., in the Request URI or Via header) matches a particular outside address/port, the enclave-fronting SBC shall replace the outside-address/port value with the original inside-address/port value and shall forward the request to the associated EI.

d. The enclave fronting SBC shall support the inclusion of provisioning information for the EI to include the location of the serving LIS.

SBC-000100 [**Required**: **SBC**] [Ref UCR: SCM-005710] For the routing of SIP signaling exchanged between EIs and the centralized ESC, the ESC-fronting SBC shall maintain a persistent TLS connection with the ESC and with the enclave-fronting SBC at each EI-hosting enclave within the Enterprise Service Area.

4.7 SC/SS

The SC shall meet the Soft Switch Backbone SRD and the UCR 2013, Change 2 requirements, with the following changes.

4.7.1 SC Requirements

SC-00071 [Required: SC] The SC shall support commercial SIP in accordance with IETF RFC 6261. This requirement replaces the need for the SC to support Assured Service SIP (AS-SIP) as defined in UCR 2013, Change 2.

SC-00081 [Required: SC] The SIP EI or SC shall query via HELD the LIS for the EI location data.

SC-00091 [Required: SC] The SC shall support location URI in the SIP INVITE using PIDF-LO location header.

5 APPENDIX A - ACRONYM GLOSSARY

AEI	Assured End Instrument
APL	Approved Product List
AS-SIP	Assured Service-Session Initiation Protocol
BCF	Border Control Function
CAC	Common Access Card
CSPR	Core Session Policy Router
CSS	Capability Summary Strings
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name Service
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DSCP	Differentiated Service Code Point
DTMF	Dual Tone Multi-Frequency
ECC	Emergency Communications Center
ECRF	Emergency Call Routing Function
EI	End Instrument
ESC	Enterprise Session Controller
ESInet	Emergency Services IP Network
ESRP	Emergency Services Routing Proxy
FQDN	Fully Qualified Domain Name
FIPS	Federal Information Processing Standards
HELD	HTTP Enabled Location Delivery
IAW	In Accordance With
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force

IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU-T	International Telecommunication Union-Telecommunications
LIS	Location Information Server
LNP	Local Network Protection
LoST	Location-to Service Translation
LPG	Legacy PSAP Gateway
MIB	Management Information Base
MILDEP	Military Departments
MOS	Mean Opinion Score
MPG	Mission Partner Gateway
MTU	Maximum Transmission Unit
NAT	Network Address Translation
ND	Neighbor Discovery
NENA-STA	National Emergency Number Association-Standards
NNI	Network-Network-Interface
OCSP	Online Certification Status Protocol
OGC	Open Geospatial Consortium
PIDF-LO	Presence Information Data Format-Location Object
PKI	Public Key Infrastructure
PSAP	Public Safety Answering Point
PRACK	Provisional Response Acknowledgement
PSInet	Public Safety IP network
PSPR	Public Safety Policy Router
RFC	Request For Comments
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SC	Session Controller

SCIP	Secure Communications Interoperability Protocol
SI	Spatial Interface
SIP	Session Initiation Protocol
SLAAC	Stateless Address Autoconfiguration
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SRD	Systems Requirement Document
SRTCP	Secure Real-time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol
STD	Standard
STIG	Security Technical Implementation Guide
STIR/SHAKEN	Secure Telephone Identity Revisited/Signature-based Handling Information Using toKENs
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UCR	Unified Capabilities Requirements
USGv6	United States Government version 6
UDP	User Datagram Protocol
URI	Uniform Resources Identifier
WFS	Web Feature Service
XML	Extensible Markup Language

6 APPENDIX B - SUPPORTED STANDARDS

Below are the standards used in this document.

Req	Standard	Standard Name / Description	Org.	Element(s)	Region (s)
C	DOD Cloud Computing Security Requirements Guide (SCCA).1 rel 3. s.l.	Department of Defense Cloud Computing Security Requirements Guide (SCCA) version 1, release 3 DOD, 2017	DISA	ALL	ALL
C	RFC 5222	LoST: A Location-to-Service Translation Protocol	IETF	CSPR, PSPR, PSAP	CONUS
C	RFC 5985	HTTP-Enabled Location Delivery (HELD)	IETF	PSPR, LIS	ALL
C	RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3	IETF	ALL	ALL
C	RFC 3261	SIP: Session Initiation Protocol	IETF	ALL	ALL
C	NENA-STA-010.3-2021	Detailed Functional and Interface Standards for the NENA i3 Solution	NENA	ALL	CONUS
C	NENA-STA-005.1.2-2022	NENA Standards for the Provisioning and Maintenance of GIS data to ECRFs and LVFs	NENA	PSPR, CSPR, LIS, PSAP	CONUS
C	NENA-STA-006.2-2022	NENA Standard for NG9-1-1 GIS Data Model	NENA	PSPR, CSPR, LIS, PSAP	CONUS

Req	Standard	Standard Name / Description	Org.	Element(s)	Region (s)
C	TWG-11 (SIP Forum)	SIP-PBX / Service Provider Interoperability "SIPconnect 2.0 Technical Recommendation"	SIP Forum	ALL	ALL
M	3GPP TR 21.916	3GPP Release 16. Updated 5G Positioning Standards plus LTE and 3G technologies	3GPP	MPG, SBC	OCONUS
M	3GPP TS 26.114	Describes the Media variations per ETSI TS 103 479	3GPP	CSPR, PSPR, SBC, PSAP	ALL
M	ATIS J-STD-110	Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification Release 2	ATIS	CSPR, PSPR, SBC, PSAP	CONUS
M	ATIS J-STD-036	Enhanced Wireless 9-1-1 Phase II	ATIS	MPG, SBC	CONUS
M	DODI 8530.01	Cybersecurity Activities Support to DOD Information Network Operations	DOD	ALL	ALL
M	DODI 8330.01.02	Department of Defense Instruction 8330.01.02, Interoperability of Information Technology (IT), Including National Security Systems (NSS); 11 DEC 2019	DOD	ALL	ALL
M	FAR 2.101	Federal Acquisition Regulation 2.101, July 2021	DOD	ALL	ALL

Req	Standard	Standard Name / Description	Org.	Element(s)	Region (s)
M	ETSI TS 103 479 v1.1.1	Emergency Communications (EMTEL); Core elements for network independent access to emergency services	ETSI	PSPR, CSPR, LIS, LDB, PSAP	OCONUS
M	2019. FIPS PUB 140-3	FIPS 140-3 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES	FIPS	ALL	ALL
M	RFC 5139	Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO) Replaces RFC 4119	IETF	PSPR, CSPR, LIS, SBC, PSAP	ALL
M	RFC 8740	Using TLS 1.3 with HTTP/2 See RFC 7841	IETF	ALL	ALL
M	RFC 6960	X.509 Internet Public Key Infrastructure Online Certification Status Protocol (OCSP)	IETF	ALL	ALL
M	RFC 6749 OAuth 2.0	OAuth 2.0 Framework	IETF	ALL	ALL
M	RFC 5245	Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols (for dual stack IPv4 - IPv6 implementation)	IETF	CSPR, PSAP, SBC	ALL
M	RFC 6947	The Session Description Protocol (SDP) Alternate Connectivity (ALTC) Attribute	IETF	CSPR, PSAP, SBC	ALL

Req	Standard	Standard Name / Description	Org.	Element(s)	Region (s)
M	RFC 7540	Hypertext Transfer Protocol Version 2 (HTTP/2)	IETF	ALL	ALL
M	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	IETF	ALL	ALL
M	RFC 5246	The Transport Layer Security (TLS) Protocol, Version 1.2. (Note: Anticipated to be used with legacy systems for interconnection only. Version 1.3 (RFC 8446) is to be the launch standard for GPSC)	IETF	ALL	ALL
M	ITU-T X.509:2005	ITU-T-X.509:2005 - X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks	IETU	ALL	ALL
M	NENA-STA.024.2021	Emergency Incident Data Object Conveyance (EIDO Conveyance)	NENA	PSAP	CONUS
M	NENA-STA.021.2021	Emergency Incident Data Object (EIDO)	NENA	PSAP	CONUS
M	NENA STA-023.2022	Next-Generation PSAP (NG-PSAP) – Date still TBD but before EOY22	NENA	PSPR, CSPR, PSAP	ALL
M	NENA-STA-005.1.1- 2017	NENA Standards for the Provisioning and Maintenance of GIS data to SBC and LVFs	NENA	CSPR, PSPR,	ALL

Req	Standard	Standard Name / Description	Org.	Element(s)	Region (s)
M	NENA STA-015.10-2018	NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping	NENA	PSPR, CSPR, LIS, PSAP	ALL
M	NENA-STA-006.1.1-2020	NENA Standard for NG9-1-1 GIS Data Model	NENA	ALL	ALL
M	NENA-STA-004.1.1-2014	NENA Next Generation United States Civic Location Data Exchange Format (CLDXF) – Update coming in Q4 FY2022	NENA	PSPR	CONUS
M	71-501	Synchronizing Geographic Information System Databases with MSAG & ALI Information Document	NENA	PSPR	CONUS
M	NENA-STA-031.1-2021	ESInet-PSBN Interconnection Standard	NENA	MPG, CSPR	CONUS
M	75-001	Security for Next-Generation 9-1-1 Standard (NG-SEC)	NENA	CSPR	CONUS
M	SAML 2.0	Security Assertion Markup Language (SAML) V2.0 Technical Overview	OASIS	CSPR	ALL
M	OMA-TS-ULP-V2_0	UserPlane Location Protocol, Version 2.0, Open Mobile Alliance	OMA	MPG	OCONUS
O	OMA-AD-SUPL-V2_0	SUPL Architecture Document, Version 2.0, Open Mobile Alliance	OMA	MPG	OCONUS

Req	Standard	Standard Name / Description	Org.	Element(s)	Region (s)
O	OMA-RD-SUPL-V2_0	SUPL Requirements Document, Version 2.0, Open Mobile Alliance	OMA	MPG	OCONUS
O	OMA-TS-ILP-V2_0	UserPlane Location Protocol, Version 2.0, Open Mobile Alliance	OMA	MPG	OCONUS
O	OMA-AD-LOCSIP-V1_0-20120117-A	Location in SIP/IP core Architecture Approved Version 1.0 – 17 Jan 2012	OMA	CSPR	OCONUS
	FCC – Legal and Regulatory Framework for NG911 Services		FCC	ALL	ALL
	SIP Forum Document Number: TWG-11	SIPconnect 2.0 Technical Recommendation	SIP Forum	ALL	ALL
	DODI 8100.04	Unified Capabilities	DOD CIO	ALL	ALL
	DODI 8010.01	DODIN Transport	DOD CIO	ALL	ALL
	DODD 8422.01E	Public Safety Communications	DOD CIO	ALL	ALL

7 APPENDIX C – CALL FLOW DIAGRAMS

This appendix contains notional ladder diagrams to show expected behaviors across various fielding conditions. These drawings are information and non-exhaustive and are meant to assist in testing.

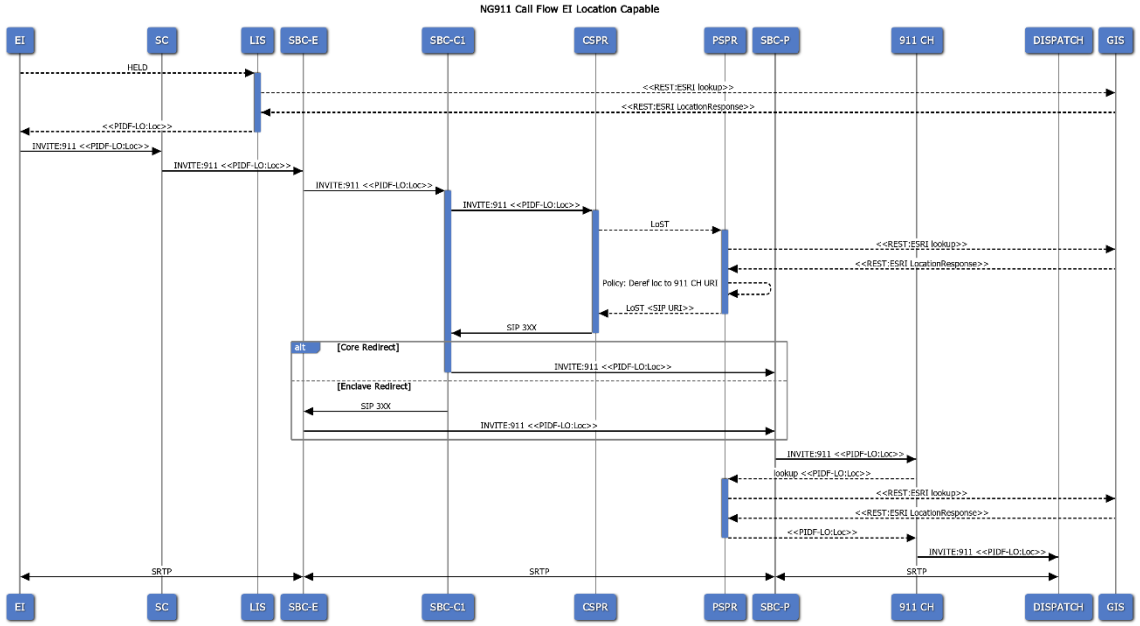


Figure 3. - SIP Location Capable End Instrument

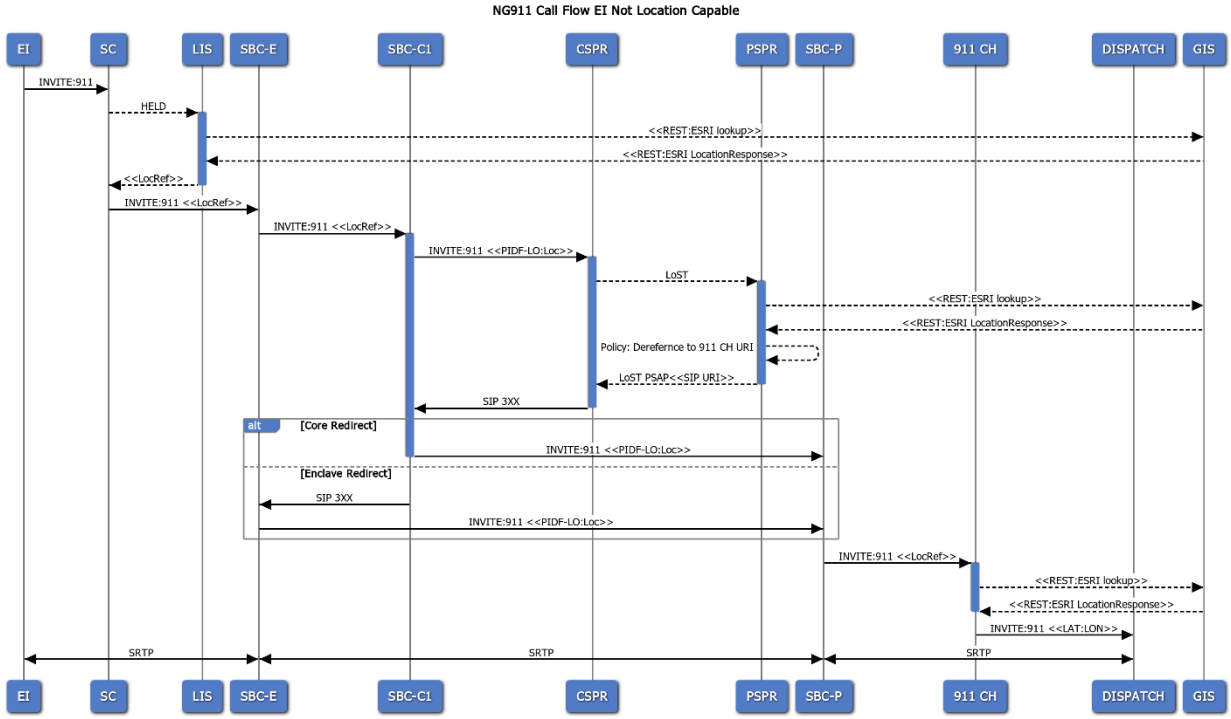


Figure 4. - Legacy Analog/Digital/SIP EI Location Inserted by LSC

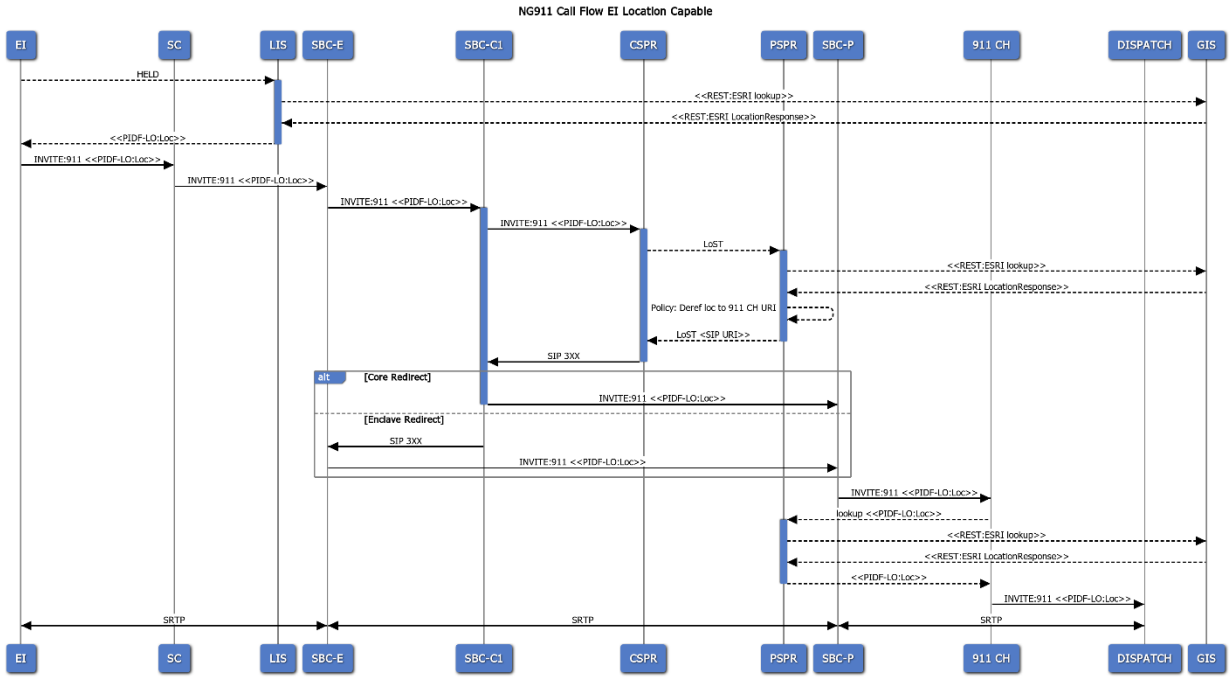


Figure 5. - Location inserted by SBC in RSC Architecture

8 APPENDIX D – FUNCTIONAL REQUIREMENTS DOCUMENT (FRD) FOR PUBLIC SAFETY COMMUNICATIONS, VOLUME 1

Nothing in this issuance shall infringe on the Department of Defense (DoD) Office of Inspector General's (OIG's) statutory independence and authority as articulated in the Inspector General (IG) Act of 1978, as amended, 5 U.S.C. App [1]. In the event of any conflict between this issuance and the DoD OIG's statutory independence and authority, the IG Act takes precedence.
When making plans for first responders to access the Mark Center Campus, coordination with the Pentagon Force Protection Agency (PFPA) is required so that first responders can access the building/campus.

Appendix D1 – Architecture

Requirement ID	Category	Requirement	Threshold/Objective
ARC-1	Architecture	The architecture shall provide connectivity for any agency to communicate with any other agency or service on any of the interconnected Emergency Services Internet Protocol Networks (ESInets).	
ARC-2	Architecture	The architecture shall provide connectivity for call signaling, media and service discovery, invocation, and management.	
ARC-3	Architecture	The architecture shall provide a service whereby all calls shall be answered by i3 Public Safety Answering Points (PSAPs) as IP (e.g., Session Initiation Protocol [SIP]) via gateways connecting non-IP-based callers.	
ARC-4	Architecture	The architecture shall provide call routing and location validation functions, which are used by the origination network. Origination networks can be built using a generic SIP architecture, or an IP Multimedia Subsystem (IMS)-based SIP architecture.	
ARC-5	Architecture	The architecture shall provide emergency service for calls which may originate from many different kinds of devices and services, to include multimedia (i.e., audio, video, text).	
ARC-6	Architecture	The architecture shall provide for emergency calls that are destined to be answered at the i3 PSAP, and may originate as either legacy or IP-based calls.	

Requirement ID	Category	Requirement	Threshold/Objective
ARC-7	Architecture	The architecture shall provide for all calls signaled with SIP audio, video, interactive text, and/or instant messaging media. PSAPs may support other protocols, or signaling gateways may be provided within the ESInets to accept other protocols and convert the signaling to SIP.	
ARC-8	Architecture	The architecture shall provide for the lifecycle of a call to include: call origination; call abandonment or completion; call duration; call clearing; and post-call processing of indefinite duration.	
ARC-9	Architecture	The architecture shall provide for the following protocol standards: call signaling; media flows; location acquisition and conveyance to the ESInet; distinguishing an emergency call from other calls; and emergency call routing protocols to the correct PSAP.	
ARC-10	Architecture	The architecture shall provide a Location-by-Value (LbyV), which is defined as location information readily consumable by the recipient of the location without transformation.	
ARC-11	Architecture	The architecture shall provide a Location-by-Reference (LbyR), which is defined as a Uniform Resource Identifier (URI) that, when dereferenced in the correct manner by an authenticated and authorized entity, shall yield the location value of the endpoint.	
ARC-12	Architecture	The service shall provide a signaling protocol primarily based on SIP.	
ARC-13	Architecture	The service shall provide for media streams transported using the Real-Time Protocol (RTP).	
ARC-14	Architecture	The service shall provide for Session Description Protocol (SDP) carried within the SIP signaling to describe how the RTP streams are established between endpoints.	

Requirement ID	Category	Requirement	Threshold/Objective
ARC-15	Architecture	The service shall include SIP URIs, which look like email addresses (e.g., sip:alice@example.com).	
ARC-16	Basic Services Intra-ESInet Routing	The service shall provide the ability for calls to other agencies within the ESInet to follow normal SIP (RFC3261 [2]) routing mechanisms. All inter-ESInet calls SHALL use Transport Layer Security (TLS).	

Appendix D2 – Call Flow

Requirement ID	Category	Requirement	Threshold/Objective
CF-1	Call Flow	The service shall provide for a Border Control Function (BCF), which provides front-line defense against deliberate attack on the ESInet.	
CF-2	Call Flow	The service shall provide processing of incoming INVITE transaction at a BCF.	
CF-3	Call Flow	The service shall provide port firewall by only permitting SIP connections to RFC5060 [3] and Secure SIP (SIPS) connections to RFC5061 [4].	
CF-4	Call Flow	The service shall provide pinhole firewall for media via inspection of SDP with opening of pinhole firewalls for authorized media streams.	
CF-5	Call Flow	The service shall provide SIP protocol repair via inspection of SIP messages for conformance to RFC3261 [2] with editing of messages that do not conform. It is RECOMMENDED that this function attempt to pass calls in all cases, rather than rejecting calls for not being RFC3261 [2] compliant.	
CF-6	Call Flow	The service shall provide Denial-of-Service (DoS) mitigation by detecting known and symptomatic DoS attacks, and filter attack attempts out of further processing. This includes Transport Control Protocol (TCP), User Dataram Protocol (UDP), and SIP attack mitigation.	
CF-7	Call Flow	The service shall provide processing of an incoming INVITE transaction at a non-terminal Emergency Services Routing Proxy (ESRP).	
CF-8	Call Flow	The ESRP shall extract location data from the call. If location is not present, skip to step 3 and use a provisioned default mapping as the Request-URI.	
CF-9	Call Flow	The ESRP shall map the location using Location-to-Service Translation (LoST). The ESRP shall maintain a persistent TLS/TCP connection to the Emergency Call Routing Function (ECRF) for this purpose. The ESRP credentials used for the TLS authentication identifies the ESRP as an authorized internal routing element within the ESInet, and the route obtained from this step shall be a lower level ESRP.	
CF-10	Call Flow	The ESRP shall perform call congestion control processing per ESRP and PSAP policy. The resulting URI becomes the Request URI for the next hop.	
CF-11	Call Flow	The ESRP shall add a "VIA" header per RFC3261 [2].	
CF-12	Call Flow	The ESRP shall inspect the INVITE for the presence of a Call Identifier, which shall be in the form of a Globally Unique Identifier (GUID), and include it in the outgoing message.	
CF-13	Call Flow	The ESRP shall add a Record-Route header per RFC3261 [2], if desired, and route the call using the procedures specified in RFC3261 [2].	
CF-14	Call Flow	The ESRP shall provide persistent TLS connections to downstream proxies.	

CF-15	Call Flow	The ESRP shall provide processing of an incoming INVITE at a terminal ESRP, which shall accept calls per RFC3261 [2] procedures. The proxy shall add a "VIA" header. The PSAP RP shall accept TLS connections. All Record-Route requests shall be honored. There are no other EXTERNAL interface requirements.	
CF-16	Call Flow	The service shall provide Policy Routing Function (PRF), which shall be applied to determine the next hop of the call.	
CF-17	Call Flow	The service shall provide PRFs, to include the following inputs: location; time of day; PSAP state (e.g., out of service, congested, disaster, under attack); and caller classification (e.g., mobile/fixed, business/residential).	
CF-18	Call Flow	The service shall provide a policy decision in the form of a URI to the next hop, which may be an intermediate ESRP or a terminal ESRP at the PSAP.	
CF-19	Call Flow	The service shall provide for processing of outgoing INVITE transactions at BCFs and non-terminal ESRPs.	
CF-20	Call Flow	The service shall provide for outgoing INVITE transactions, which shall follow procedures in RFC3261 [2]; "VIA" headers shall be added. Proxies SHALL NOT hide or modify Via headers. Record Route's SHALL be honored by all elements. TLS SHALL be used within the ESInet, and SHALL be used with downstream proxies. An outgoing call MAY have an Incident Identifier and SHALL have a Call Identifier.	
CF-21	Call Flow	The service shall provide for Public Switched Telephone Network (PSTN) Call Origination presented to an IMS-based ESInet.	
CF-22	Call Flow	The service shall support Joint Interoperability Test Command (JITC)-approved, direct interconnect to DoD voice switches for SIP- and Time-Division Multiplex (TDM)-based Call Origination from government landlines and extensions.	

Appendix D3 – Service Creation

Requirement ID	Category	Requirement	Threshold/Objective
SC-1	Service Creation	The service shall provide an abstract interface that defines the messages and message exchange patterns (i.e., operations) involved in interacting with the service.	
SC-2	Service Creation	The service shall provide one or more concrete interfaces, each of which defines a binding of the abstract interface. Each binding shall specify a specific protocol and data format that implements the abstract interface.	
SC-3	Service Creation	The service shall provide one or more service end points (i.e., ports), each of which shall associate a concrete interface with a URI that a service requester can use to interact with a service instance.	
SC-4	Service Creation	The service shall provide Service Registration and Discovery on the concept of a generally accessible service registry that hosts the service definitions for all available services.	
SC-5	Service Creation	The service shall provide Service Definitions to the service registry. Each registered service shall include administrative (i.e., provider identity), as well as technical (i.e., service contract) information about the service.	
SC-6	Service Creation	The service shall provide a Service Registry, which is a database of finding a given service formulating a query with appropriate search criteria values using a standardized API. Once the service is found, one or more subsequent queries are used to retrieve service contract information.	
SC-7	Service Creation	The service shall provide Interacting with services in which the service requester knows the service end point URI. A service contract includes an end point definition, which associates a URI to a binding (i.e., to a specific protocol and data format).	
SC-8	Service Creation	The service shall provide service Method Exchange Pattern (MEP) interactions that are asynchronous (e.g., notification, solicit MEPs) or synchronous (e.g., request-reply, one-way, fire-and-forget MEPs). Note that some concrete interfaces may not natively support certain MEPs due to limitations of the underlying protocol.	
SC-9	Service Creation	The service shall provide Service Termination, which builds on a notification MEP wherein a service requester receives asynchronous “service up” status notifications at regular intervals. The service requester behavior then interprets missing notifications as an indication of service failure. For this to work, a service requester needs to explicitly tell the service provider which consumer-side end point URI to send service status notifications.	

Appendix D4 – Basic Services Data Associated with a Call

Requirement ID	Category	Requirement	Threshold/Objective
B-1	Basic Services Data Associated with a Call	The service shall provide data associated with the call in an XML data structure retrieved from a web service, to be operated by the origin network or a contractor.	
B-2	Basic Services Data Associated with a Location	The service shall provide a location in an XML data structure retrieved from a web service.	
B-3	Basic Services Data Associated with a Caller	The service shall provide data associated with a caller in an XML data structure retrieved from a web service, which shall include a header containing the URI for the data associated with the caller.	
B-4	Basic Services Logging	The service shall provide the ability for call and data Logging. Every Call for Service (CFS) event occurring on the ESInet SHALL be logged on the service. Log Events include: any incident related media; data and time stamp; agency; agent (if appropriate); call and Incident IDs (if appropriate); and an Event Type.	

Appendix D5 – Event Notification

Requirement ID	Category	Requirement	Threshold/Objective
EN-1	Event Notification	The service shall exchange and share information following various interaction models, most of which shall involve a producer entity (i.e., source of the information), and one or more consumer entities.	
EN-2	Event Notification	The service shall provide an Automatic Location Identification (ALI) query, which is typically a database readily available to a producer. Consumers shall request (i.e., pull) the information from the producer when they need it.	
EN-3	Event Notification	The service shall provide the ability for a producer of information to asynchronously push location-sensitive event information to consumers as it becomes available (e.g., Amber Alerts only relevant to a certain jurisdiction).	
EN-4	Event Notification	The service shall match consumers with producers. Before a producer can start propagating event information to one or more consumers, it has to know which consumers are interested in receiving such information.	
EN-5	Event Notification	The service shall provide an Event Topics Registry.	
EN-6	Event Notification	The service shall provide the following Registry Entries: Event Topic; Standard Topic; Reference to Event semantics; Key words list; XML namespace URI of event information; Policy statements about publisher and consumer relationships; and URI list of children Event Topics.	
EN-7	Event Notification	The service shall provide a Publisher Registry, which serves as a directory for all ESInet event publishers.	
EN-8	Event Notification	The service-provided Registry entries shall be as follows: Publisher name/ID; Publisher type service; agency; Complementary publisher metadata; List of supported ESInet event topics; Technology identifier; End Point Reference; and Service Area for publishers that serve location-sensitive events.	
EN-9	Event Notification	The service shall provide Event Notification Messages.	
EN-10	Event Notification	The service shall provide Advanced Event Notification mechanisms.	
EN-11	Event Notification	The service shall provide for location-sensitive events (e.g., tornado warnings) that affect a specific service area. Such events shall only be sent to agencies that subscribe to the event topic.	

Appendix D6 – Security

Requirement ID	Category	Requirement	Threshold/Objective
SEC-1	Security	The service shall provide security for the entire path from sender to recipient by equivalent security means—as in TLS (RFC4346 [5])—and shall be used for all communications on the ESInet.	
SEC-2	Security	The service shall provide Authentication by implementing strong authentication for their agents by employing two or three factor smartcards, passwords, and/or biometrics.	
SEC-3	Security	The service shall use between agencies Security Assertion Markup Language (SAML). To the extent possible, all services and facilities in the ESInet shall provide "Single Sign On" using SAML.	
SEC-4	Security	The service shall provide a source of credentials for authentication. The PSAP Public Key Infrastructure (PKI) shall provide a public key certificate to each PSAP and to service providers providing services on one or more ESInet(s).	
SEC-5	Security	The service shall provide Certificate Policies.	
SEC-6	Security	The service shall provide Certificate Revocation Lists.	
SEC-7	Security	The service shall provide Authentication using TLS.	
SEC-8	Security	The service shall provide Authentication using Web Services.	
SEC-9	Security	The service shall provide Authentication using SIP.	
SEC-10	Security	The service shall provide Authorization by SAML 2.0. Profile of Extensible Access Control Markup Language Version 2.0 (XACML 2.0) [6] shall be used to control access and provide at least one Policy Store conformant to XACML 2.0 using the Lightweight Directory Access Protocol (LDAP) profile for distribution of XACML policies.	
SEC-11	Security	The service shall provide Integrity Protection of messages by implementing SHA-256.	
SEC-12	Security	The service shall provide Privacy. The standard method for privacy protection of messages in i3 is Advanced Encryption Standard (AES) (Federal Information Processing Standards-Publication [FIPS-PUB]-197 [7]).	
SEC-13	Security	The service shall provide Non-Repudiation. The mechanism to accomplish such Non-Repudiation shall be a digital signature using an XML-Signature (RFC3275 [8]) with credentials.	
SEC-14	Security	A change-control process shall be implemented to ensure that the system configuration is in its approved state.	
SEC-15	Security	The service shall meet applicable Cybersecurity (CS) Risk Management Framework requirements, and receive an Authority to Operate (ATO)/Authority to Connect (ATC). The system shall be configured to be audited, or otherwise verified, on a regular basis to determine the continued validity of the ATO/ATC.	

Appendix D7 – Service Management

Requirement ID	Category	Requirement	Threshold/Objective
SM-1	Service Management	The service shall provide Provisioning. The i3 standard provisioning mechanism is Service Provisioning Markup Language (SPML), Version 2.0 [9].	
SM-2	Service Management	The service shall provide Remote Telecommunicator management.	
SM-3	Service Management	The service shall provide Routing management. The route database for i3 is the LoST mapping database.	
SM-4	Service Management	The service shall provide Alarms. Simple Network Management Protocol (SNMP) is the standard mechanism in i3 for reporting alarm conditions from network equipment across the ESInet.	
SM-5	Service Management	The service shall provide Reports (i.e., Logging). Generic log record includes: Record ID; Timestamp; Source; Call ID; Incident ID; and Record Type. The body of the record is an XML data structure defined by the Record Type schema.	
SM-6	Service Management	The service shall provide Voice over Internet Protocol (VoIP) quality metrics. User Agents shall log Real-Time Transport Control Protocol (RTCP) reports for calls, and PSAP systems shall have collection and reporting mechanisms for these statistics.	

Appendix D8 – Roles and Responsibilities

Requirement ID	Category	Requirement	Threshold/Objective
RR-1	Roles and Responsibilities	The service shall provide Agencies, which include the following: access network operator; calling network operator; State emergency communications agency; regional emergency communications agency; and 9-1-1 Authority.	
RR-2	Roles and Responsibilities	The service shall provide a Functional Element Responsible Agency. Regional emergency communications agencies operate a region, while State emergency communications agencies may operate a State-wide backbone, and a Federal agency may operate a National backbone network safety network.	
RR-3	Roles and Responsibilities	The service shall provide a Location Information Server (LIS) where the access network is responsible for providing the service and the data it contains.	
RR-4	Roles and Responsibilities	The service shall provide a PSAP, which is responsible for accepting calls routed to it by entry or intermediate ESRPs, and transferring calls to secondary PSAPs. The PSAP is responsible for creating the local policies used by ESRPs to route calls to it, and communicating such policies to the appropriate ESRP(s).	

Appendix D9 – Profile Minimal-Profile Definition

Requirement ID	Category	Requirement	Threshold/Objective
PMPD-1	Profile Minimal-Profile Definition	The service shall provide guidelines and clarifications on how a related set of technologies and/or standards shall be used together.	
PMPD-2	Profile Minimal-Profile Definition	The service shall provide definitions of specific subsets of system features and/or interfaces.	
PMPD-3	Profile Minimal-Profile Definition	The service shall provide a Profile or Conformance Profile, which adheres to the implicit or explicit requirements (i.e., mandatory, optional, conditional) within that Profile on specific external interfaces and functional requirements.	
PMPD-4	Profile Minimal-Profile Definition	The service shall provide Conformance Profiles for both sides of external interfaces, and two conforming implementations shall interoperate when connected together. Profiles defined for common realizations expected in i3 implementations include: ESRPs; LoST servers (e.g., ECRF, LVF and Root Discovery Service); Firewall/BCF; Wireline Gateway; Wireless Gateway; etc.	

Appendix D10 – Call Handling/CAD Event Creation

Requirement ID	Category	Requirement	Threshold/Objective
CHEC-1	Call Handling/ CAD Event Creation	The service shall provide a Computer-Aided Dispatch (CAD) process by reporting an incident to a PSAP.	
CHEC-2	Call Handling/ CAD Event Creation	The service shall provide specific instructions to be associated PSAP with CAD event types.	
CHEC-3	Call Handling/ CAD Event Creation	The service shall display specific questions regarding the nature of the incident (i.e., type) thereby assisting in creating a better classification of the incident.	
CHEC-4	Call Handling/ CAD Event Creation	The service shall provide Special CAD Incident Types, and the selected method shall be compatible with the local agency's requirements. Some examples of typical user-definable specialized incident types include: hazardous materials; Weapons of Mass Destruction (WMD); decontamination; bomb threat; and civil disturbance.	
CHEC-5	Call Handling/ CAD Event Creation	The service shall provide Advised Events. This creates the ability to record information from citizens about particular situations or events that do not require the dispatching of any public safety resources.	
CHEC-6	Call Handling/ CAD Event Creation	The service shall provide Make Paper Events. This is the ability to enter an event that bypasses dispatch, but assigns a resource with a disposition and closes the event upon entry with the user designated disposition.	
CHEC-7	Call Handling/ CAD Event Creation	The service shall allow for System Administrator-defined CAD incident types or nature codes.	
CHEC-8	Call Handling/ CAD Event Creation	The service shall allow system users to modify the incident type and provide new/updated response plan information/suggestions based on the new incident type.	
CHEC-9	Call Handling/ CAD Event Creation	The service shall provide the capability to create an event, assign a unit, and close the event with a disposition without going through the dispatch process steps.	
CHEC-10	Call Handling/ CAD Event Creation	The service shall provide the capability to flag a CFS as an "Advised Event" separate from the incident type/nature code.	

CHEC-11	Call Handling/ CAD Event Creation	The service shall provide a Determine Dispatch Need, which is where a decision is made that resources are required, then the collected information shall be routed to a dispatch position to begin the resource assignment process.	
CHEC-12	Call Handling/ CAD Event Creation	The service shall utilize Incident Disposition. The CAD system shall have end user-configurable settings to manage the closure of an incident. This ability shall include the capability to automatically close an event if the received Mobile Data Computer (MDC) data indicates the incident is complete by determining resources are no longer assigned to the incident.	
CHEC-13	Call Handling/ CAD Event Creation	The service shall assign Incident Classification and Priority. The process determines the appropriate dispatch and response needs with the incident classification. The process shall be able to be upgraded or downgraded as the incident details depict.	
CHEC-14	Call Handling/ CAD Event Creation	The service shall be able to Check for Duplicate incidents.	
CHEC-15	Call Handling/ CAD Event Creation	The service shall provide a CAD system that is ergonomically structured and easy flowing, with a Graphical User Interface (GUI) that can be used to enter and/or validate incident-related information.	
CHEC-16	Call Handling/ CAD Event Creation	The service shall Determine Capture Locations by providing an automated means for loading all location and location-related information available into the CAD event record from the system on which the 9-1-1 call was made, without requiring the information to be manually re-entered.	
CHEC-17	Call Handling/ CAD Event Creation	The service shall provide Location Verification. CAD systems shall contain an easily-invoked tool to assist users in validating entered locations and shall include prompts, or ordered lists, which present the user with suggested addresses/locations when the exact address cannot be validated.	
CHEC-18	Call Handling/ CAD Event Creation	The service shall provide the Retrieval of Incoming Calls. CAD systems shall be interfaced to the 9-1-1 call handling system to facilitate the automatic passing of the call data—to include ALI/Automatic Number Identification (ANI) data—to the CAD system.	
CHEC-19	Call Handling/ CAD Event Creation	The service shall provide CAD users the capability to create a new CFS event. A CFS event can be created by a call taker, dispatcher or responding resource, depending on the source of the request.	
CHEC-20	Call Handling/ CAD Event Creation	The service shall provide a Determining Response Agency and Service Area. CAD systems shall use the event's validated location information (e.g., civic location, X/Y coordinate, street intersections) to determine the response area for each service agency involved.	

CHEC-21	Call Handling/ CAD Event Creation	The service shall provide Alarm Monitoring, as defined in Vol. II, Appendix O – Incident Disposition.	
CHEC-22	Call Handling/ CAD Event Creation	The service shall provide CAD Event Routing. Certain high priority incidents (e.g., cardiac arrest, bank robbery in progress, active shooter) need to have emergency responders assigned and dispatched as quickly as possible. In these situations, as soon as the call taker obtains the incident type and validates the incident's location, the CFS event(s) shall be transferred (i.e., routed) to the appropriate dispatch positions so emergency responders can be assigned and dispatched.	

Appendix D11 – Dispatch Support

Requirement ID	Category	Requirement	Threshold/Objective
DS-1	Dispatch Support	The service shall provide the ability to route to a Decision Dispatcher. The dispatcher is responsible for using the CAD system, in multiple ways, to manage an incident.	
DS-2	Dispatch Support	The service shall provide Run Cards/Response Plans. Response Plans identify the number, type or specific units that respond to an incident of a specific type, and the order in which they respond.	
DS-3	Dispatch Support	The service shall provide Adjustable Dispatch Levels. This refers to changing dispatch levels to alternative sets of dispatch policy plans in special circumstances (e.g., inclement weather, major incidents, disasters, Mass Casualty Incidents (MCIs), acts of terrorism, etc.).	
DS-4	Dispatch Support	The service shall provide Additional Attributes that have the ability to allow dispatchers to modify attributes on-the-fly and be dynamic. The system shall also provide a way to search for attributes.	
DS-5	Dispatch Support	The service shall provide Unit Attributes (e.g., engine ladder, aid car, medic, fire boat, patrol, Special Weapons and Tactics [SWAT], etc.).	
DS-6	Dispatch Support	The service shall provide Personnel Attributes (e.g., communication, Emergency Medical Technician [EMT]/paramedic, SWAT, hostage negotiator, etc.).	
DS-7	Dispatch Support	The service shall provide Mutual Aid Function. The CAD system formulates resource recommendations based on another agency's resources, availability, and location. This is frequently based upon Memorandum of Understanding (MOU) agreements with other agencies.	
DS-8	Dispatch Support	The service shall provide Automatic Aid Function. The CAD system within one agency formulates resource recommendations based upon the location and availability of a different agency's resources. Resources can be automatically dispatched. Automatic, cross-agency dispatching normally requires a real-time CAD-to-CAD interface.	
DS-9	Dispatch Support	The service shall be configurable to provide Unit Rotation (i.e., Unit Load Balancing), which run assignments adjusted by the CAD system to give rest to busy units and assigns incidents to less-active units.	
DS-10	Dispatch Support	The service shall provide Conditional Availability of Apparatus, allowing units with specific statuses to be recommended and dispatched to certain types of incidents.	
DS-11	Dispatch Support	The service shall provide Special Dispatch Areas. This is a geographic area for which a non-standard resource (i.e., unit) response is desired. Examples of these areas include: flooded areas, restricted access areas, and civil disturbances.	
DS-12	Dispatch Support	The service shall provide a CAD system that defines special dispatch area types and assign each a unique identifier.	

DS-13	Dispatch Support	The service shall assign a special dispatch area type to CAD geo-file addresses, intersections, and blocks for each service agency.	
DS-14	Dispatch Support	The service shall specify a non-standard response for a location identified with a special dispatch area type.	
DS-15	Dispatch Support	The service shall define non-standard responses as being applicable only during certain days of the week and/or times of the day.	
DS-16	Dispatch Support	The service shall provide the capability that if one or more non-standard responses are defined, but none of them are applicable, then the standard response is employed.	
DS-17	Dispatch Support	The service shall provide for Emergency Medical Dispatch and Incident Triage.	
DS-18	Dispatch Support	The service shall allow for customization based on the needs of the agency (e.g., medical direction, operations).	
DS-19	Dispatch Support	The service shall provide a CAD system designed to assist the call taker in identifying the type of incident, resources needed, and level of response.	
DS-20	Dispatch Support	The service shall provide the capability to allow a unit to be dispatched to the incident as soon as the address is confirmed.	
DS-21	Dispatch Support	The service shall prompt the call taker to provide pre-arrival instructions to the caller or responding unit.	
DS-22	Dispatch Support	The service shall allow for recommended changes based on the information obtained and entered into the CAD program.	
DS-23	Dispatch Support	The service shall provide the capability for Channel Designations.	
DS-24	Dispatch Support	The service shall allow for a table of radio channels/talk groups.	
DS-26	Dispatch Support	The service shall allow each radio channel or talk group, as defined in the CAD system, to have an associated list of the agencies.	
DS-25	Dispatch Support	The service shall allow the radio channels or talk groups used for tactical purposes to be ranked according to the order in which they are assigned.	
DS-27	Dispatch Support	The service shall allow for tracking of the maximum number of concurrent incidents.	
DS-28	Dispatch Support	The service shall include a flag indicating a requirement for the automatic assignment of a tactical channel that can be set for each incident type in the CAD system.	
DS-29	Dispatch Support	The service shall allow for the assignment of a tactical radio channel available to units upon the dispatch.	
DS-30	Dispatch Support	The service shall allow the dispatcher to manually flag or assign one or more tactical radio channels or talk groups to an incident.	
DS-31	Dispatch Support	The service shall provide the ability to track the release and reassignment of radio channels or talk groups.	
DS-32	Dispatch Support	The service shall release the tactical channels or talk groups assigned to an incident when that incident has been cleared. The tactical channels or talk groups shall then be made available for other incidents.	

DS-33	Dispatch Support	The service shall provide an assignment of a tactical channel or talk group to an incident, and direct the radio system to have the radios associated with units assigned to the incident to be automatically switched to that tactical channel or talk group—if the radio system provides this capability.	
DS-34	Dispatch Support	The service shall have the capability to identify, upon clearing an incident, which tactical channel or talk group was assigned and confirm that the release of the channel or talk group has occurred. The service shall then direct the system to have the radios automatically revert to their previous channel or talk group selection.	
DS-35	Dispatch Support	The service shall be able to record which radio channels were patched together for an incident, including start and end times.	
DS-36	Dispatch Support	The service shall provide Be-on-the-Look-Out (BOLO) / Attempt-to-Locate Alerts.	
DS-37	Dispatch Support	The service shall provide support creation and distribution of any BOLO entered into the CAD system.	
DS-38	Dispatch Support	The service shall provide a BOLO structure, which includes all necessary information (e.g., the nature of the BOLO, priority, date, range of effectiveness, subject and/or vehicle information, hazard information, contact information).	
DS-39	Dispatch Support	The service shall allow narrative fields for additional information.	
DS-40	Dispatch Support	The service shall provide the means for BOLO information to be easily searchable, printable, and have the ability to automatically populate on an incident sheet referencing any particular name, address, or vehicle information.	
DS-41	Dispatch Support	The service shall flag the field automatically with configurable visual and audible alerts.	
DS-42	Dispatch Support	The service shall support a workflow record for initial BOLO creation and any additional edits.	
DS-43	Dispatch Support	The service shall support the optional capability of Dispatch Units to assign one incident number to each unit responding to the incident.	
DS-44	Dispatch Support	The service shall assign an incident number to each agency responding to the incident.	
DS-45	Dispatch Support	The service shall assign, for an EMS response, a Patient Care Report (PCR) number to each patient at the incident.	
DS-46	Dispatch Support	The service shall capture every time stamp associated with each unit’s response and status change related to the incident.	
DS-47	Dispatch Support	The service shall capture all status changes and their times for statistical and research purposes (e.g., out of service versus in service) to calculate “lost unit hours”.	

DS-48	Dispatch Support	The service shall provide the capability for Resource Alerting. Resource Alerting mechanisms include: MDCs in public safety vehicles; radio system tone encoders that emit tones and then activate the Public Address (PA) system; fire station alerting systems; fire station "rip and run" faxes and printers that print out incident information; alerting via email delivered to portable devices; alerting via Short Message Service (SMS) delivered to cellular telephones; and alerting via alphanumeric pagers using protocols such as Telocator Alphanumeric Protocol (TAP), Wireless communications Transfer Protocol (WCTP), Simple Mail Transfer Protocol (SMTP), and Simple Network Paging Protocol (SNPP).	

Appendix D12 – Resource Management

Requirement ID	Category	Requirement	Threshold/Objective
RM-1	Resource Management	The service shall provide Resource Management with the ability to assign and track resources.	
RM-2	Resource Management	The service shall include Resources, not only the traditional responders (i.e., law enforcement, fire, and EMS), but may also include units like animal control, tow trucks, and utility services.	
RM-3	Resource Management	The service shall provide Tracking of these resources. It is critical for the dispatcher to know what units are available to send to a particular CFS, and what their status is at any given time.	
RM-4	Resource Management	The service shall provide the ability to Move Up (e.g., "Fill-In" and "Station Fill").	
RM-5	Resource Management	The service shall recognize resource gaps that will likely result in response performance.	
RM-6	Resource Management	The service shall recommend or automatically dispatch units to move up in order to address those identified gaps.	
RM-7	Resource Management	The service shall initiate move ups based on user-defined manual or automated logic processes.	
RM-8	Resource Management	The service shall provide the ability to dynamically document that a unit is staffed or unstaffed before or after it is assigned to an incident.	
RM-9	Resource Management	The service shall provide a Cross-Staffing function within the CAD system.	
RM-10	Resource Management	The service shall be able to account for the number of qualified personnel available in a station, and determine the best possible resource allocation at any given moment from that station.	
RM-11	Resource Management	The service shall utilize any combination of dedicated or contingent staffing to most appropriately utilize resources.	
RM-12	Resource Management	The service shall account for the qualifications of personnel (e.g., fire apparatus driver/operator, EMS certification, rescue certification) to establish the best possible resource allocation based on prioritized needs for the response.	
RM-13	Resource Management	The service shall take the remaining piece(s) of apparatus out of service, when one piece of apparatus is assigned to an event—based on a single, shared crew assigned to multiple pieces of apparatus.	
RM-14	Resource Management	The service shall provide System Status Management (i.e., Dynamic Resource Deployment).	
RM-15	Resource Management	The service shall build multiple system status plans (e.g., by hour of day, day of week) that define the levels of resource availability, and which posts/stations shall be prioritized for coverage.	
RM-16	Resource Management	The service shall monitor each plan in effect, on a continuous basis, and alert the dispatcher if the plan goes "out of compliance" (i.e., units not in their proper position).	
RM-17	Resource Management	The service shall include the capability for multiple plans by unit resource type.	

RM-18	Resource Management	The service shall provide capability for Additional Unit Status. Additional Unit Status functionality is required to track resource availability.	
RM-19	Resource Management	The service shall include a list of statuses that shall be considered, to include: Assigned to Post/Move Up; En Route to Post; At Post; Available in Area of Assigned Post; and Available for Emergency Incidents Only.	
RM-20	Resource Management	The service shall provide statuses that are employed by CAD systems, to include: Staged; Patient/Incident Contact; En Route to Hospital; At Hospital; and Clear from Hospital.	
RM-21	Resource Management	The service shall be able to support modifiers for Additional Unit Status, to include: various statuses needed for unit readiness or during patient care; add parameters to the incident that relate to the response priority (e.g., lights and siren or non-emergency mode); show if a unit is Basic Life Support (BLS) or Advanced Life Support (ALS), and allow for multiple transports by the same unit on the same incident (e.g., a mass casualty incident).	
RM-22	Resource Management	The service shall provide for Strike Team/Task Force Designations.	
RM-23	Resource Management	The service shall allow the dispatcher to group units into a task force or strike team.	
RM-24	Resource Management	The service shall track, individually, all resources in the system's database and shall make a record that the resources were part of a virtual unit, so that the virtual unit response data can be easily retrieved.	
RM-25	Resource Management	The service shall support Rostering.	
RM-26	Resource Management	The service shall provide the capability to create rosters (i.e., assign personnel to a vehicle or position to facilitate on/off duty transactions).	
RM-27	Resource Management	The service shall allow the dispatcher to adjust the rosters and/or assignments (i.e., on-the-fly, during shifts, and above normal complements).	
RM-28	Resource Management	The service shall warn the dispatcher if a resource complement is below minimum.	
RM-29	Resource Management	The service shall contain a two-way, real-time interface to auto populate roster information in CAD.	
RM-30	Resource Management	The service shall support Scheduling.	
RM-31	Resource Management	The service shall provide scheduling capabilities to include pre-assignment of personnel to shifts, platoons, or beats.	
RM-32	Resource Management	The service shall allow the dispatcher, with proper permissions, to make adjustments to scheduling on-the-fly and/or during shifts.	
RM-33	Resource Management	The service shall provide Mileage Tracking.	
RM-34	Resource Management	The service shall provide Hydrant Location and Status , to include: location; service status; recent test date; flow rate; and main size.	

RM-35	Resource Management	The service shall provide Additional Unit Dispositions.	
RM-36	Resource Management	The service shall enable the CAD administrator to define a list of available unit dispositions, as well as require a disposition based on call type and jurisdiction.	
RM-37	Resource Management	The CAD system shall NOT require a disposition if agency policy does not require the use of dispositions.	
RM-38	Resource Management	The service shall support Exception Reason Tracking.	
RM-39	Resource Management	The CAD system shall allow dispatchers to record reasons when a unit has a response time that exceeds the standard.	
RM-40	Resource Management	The service shall identify and require an exception, in any case, when user-defined response time standards are not met.	
RM-41	Resource Management	The service shall establish a system administrator-defined list of exception reasons established for each CAD time interval.	
RM-42	Resource Management	The service shall provide Geo-Fencing with the ability for geo-fence creation tools that allow the use of polygons, circles, ellipses, and rectangles.	
RM-43	Resource Management	The service shall include Geo-Fencing Alerts, to include: unique visual and audible identification; resource identification; geo-fence identification; current resource position; timestamps of entry and exit of geo-fence areas; and ability to clear alerts and history from view while maintaining historic records.	
RM-44	Resource Management	The service shall provide Station Dispatch with the capability to dispatch a fire and/or EMS station to an incident, regardless of the number of units or personnel that station has assigned to it or on duty.	
RM-45	Resource Management	The service shall provide Pre-Release or Pre-Alerting, which provides advance notice to stations and/or units that an imminent dispatch is likely to occur.	
RM-46	Resource Management	The service shall provide Vehicle/Unit Change to allow system supervisors and other authorized users the ability to modify vehicle and resource capabilities, as required.	
RM-47	Resource Management	The service shall provide Automatic Driving Directions and Routing in order to advise units of the best route to respond to an incident, based upon the responding unit’s current location.	
RM-48	Resource Management	The service shall allow for Bypassed Units to automatically alert the dispatcher when a unit closer to a CFS becomes available and the currently assigned unit is en-route, but still farther away.	
RM-49	Resource Management	The service shall provide Post-Dispatch Response Re-Evaluation that has the ability to reevaluate the appropriateness of the units assigned to an incident.	

Appendix D13 – Call Incident/Event Management

Requirement ID	Category	Requirement	Threshold/Objective
CIEM-1	Call Incident/Event Management	The service shall provide Display of Incident/Event Data, which displays CFS event data on the CAD monitor after being selected by the dispatcher.	
CIEM-2	Call Incident/Event Management	The service shall provide Update Incident Status, which is the capability to record supplemental information updates in the CFS event as it is received from callers, field resources, and other sources.	
CIEM-3	Call Incident/Event Management	The service shall provide Dispatch Resource Decision to recommend resources when the resource requirement is changed based upon agency-defined procedures, workload balancing, unit capability, and proximity of the resources.	
CIEM-4	Call Incident/Event Management	The service shall Update Assigned Resources to detect when a reduction in dispatched resources is required, and recommend readjusted resources that meet the requirements of the incident.	
CIEM-5	Call Incident/Event Management	The service shall Update Supplemental Resources Tracking, allowing the ability to divide the response area into multiple zones, based on user-defined criteria, to ensure a quick response to the request.	
CIEM-6	Call Incident/Event Management	The service shall Assign Units by using drag-and-drop and point-and-click pulldown menus to also include the ability to assign one or more units to an incident with a single command.	
CIEM-7	Call Incident/Event Management	The service shall Update Incident Data by logging the following information for all entries into the CFS event: date; time; user- ID; position (i.e., terminal) ID; action performed; and any notes associated with action.	
CIEM-8	Call Incident/Event Management	The service shall provide a Records Management System (RMS) Incident/Case Number to assign to the incident for tracking purposes.	
CIEM-9	Call Incident/Event Management	The service shall have the capability to Transfer Basic Incident Data to the RMS.	
CIEM-10	Call Incident/Event Management	The service shall be able to Display Additional Incident Data by providing a notification for each entry completed. This will ensure the dispatcher is made aware of each entry for processing.	
CIEM-11	Call Incident/Event Management	The service shall be able to Reopen Incident by incident number, location, or unit ID.	
CIEM-12	Call Incident/Event Management	The service shall Add Destination Locations to have the ability to accurately track the destination of all units assigned to a particular incident in order to allow locations and activities to change throughout.	

CIEM-13	Call Incident/Event Management	The service shall provide Hospital Status / Availability and Hospital Recommendation. Note that it may be prudent to consider a third-party application interface so that information is accessible outside of the CAD system network.	
CIEM-14	Call Incident/Event Management	The service shall provide Patient Tracking in order to track EMS patients from the scene of an incident to a destination or disposition.	
CIEM-15	Call Incident/Event Management	The service shall enforce protection of health data In Accordance With (IAW) the Federal Health Information Portability and Accountability Act (HIPAA) statute and derivative regulations.	
CIEM-16	Call Incident/Event Management	The service shall be able to link an audio file to a CAD event. This function could be contained within a CAD system, or be provided via a separate recorder device interfaced with the CAD system, for the purpose of linking the recording to a particular CFS.	
CIEM-17	Call Incident/Event Management	The service shall be able to have Multiple Simultaneous Incidents assigned to a Single Unit, providing a method of assigning multiple low priority incidents to a single unit. This allows the unit to either pick from the assigned batch of CFS events, or to automatically receive information for the next incident upon closing the current incident.	
CIEM-18	Call Incident/Event Management	The service shall Schedule Events to provide the ability to automatically schedule the CFS event for future dispatch.	
CIEM-19	Call Incident/Event Management	The service shall have a Secondary Incident Location, providing the ability of the CAD system to capture, validate, and track units assigned to the same incident, but operating at different locations from the primary or initial location.	
CIEM-20	Call Incident/Event Management	The service shall provide Single Discipline Incident to a Combined Discipline Incident. This is the ability to add another agency's resources to a CFS event, as well as provide the capability to link added agency records with the initial CFS event.	
CIEM-21	Call Incident/Event Management	The service shall provide Timers to allow configuration of multiple timers based on unit status and CAD incident type (e.g., time on a particular call, time since last check-in, time at the hospital or jail).	
CIEM-22	Call Incident/Event Management	The service shall provide User Defined Status Timers, providing the ability for the system administrator to create customized, definable timers.	

Appendix D14 – Supplemental Resource Request Tracking

Requirement ID	Category	Requirement	Threshold/Objective
SRRT-1	Supplemental Resource Request Tracking	The service shall Request Supplemental Resource (e.g., utility companies, repair vehicles, animal control, Red Cross relief units, etc.).	
SRRT-2	Supplemental Resource Request Tracking	The service shall Request a Supplemental Resource Rotation List by having the ability to store—and provide for easy retrieval—a list of authorized providers of unique or supplemental supplies or services.	
SRRT-3	Supplemental Resource Request Tracking	The service shall Notify Supplemental Resource Service to provide dispatch information, by the dispatcher, about the incident to which it is requested to respond.	
SRRT-4	Supplemental Resource Request Tracking	The service shall have the ability to Enter and Update Supplemental Service Record.	

Appendix D15 – Incident Disposition

Requirement ID	Category	Requirement	Threshold/Objective
IND-1	Incident Disposition	The service shall include CAD system activities related to the closing of an incident, including: assigning case numbers; entering an incident disposition; and transferring the call data to one or more RMSs.	
IND-2	Incident Disposition	The service shall Determine Incident / Event Status, providing the ability to change the event status as the situation evolves or a resolution is achieved.	
IND-3	Incident Disposition	The service shall Utilize Incident Management, providing the ability to dynamically update the CFS event with notations, updates, status changes, and notifications.	
IND-4	Incident Disposition	The service shall Determine Report Functionality, providing the ability to automatically transfer incident/event data relevant to external RMSs or reporting systems.	
IND-5	Incident Disposition	The service shall Record Disposition to provide for the CFS event to contain the disposition of the incident. This may include a narrative in addition to the disposition type.	
IND-6	Incident Disposition	The service shall Send Data to Records Management System, providing the ability to exchange all CFS event information with an RMS.	
IND-7	Incident Disposition	The service shall Assign Agency-Specific Report Numbers to allow for both the CAD CFS Event Number and the Agency Report Numbers to be fully configurable (e.g., “1 to N,” “mmddyyxxxx,” “mmddyyhhmmssxxx,” “FY12xxxxxx,” “yy-mm-dd-xxxx”).	

Appendix D16 – Business Function/CAD Administration

Requirement ID	Category	Requirement	Threshold/Objective
BFCA-1	Business Function/CAD Administration	The CAD System Administration shall provide various administrative functions and capabilities required to keep the CAD system current and operational. This shall include: install and monitor the Operating System (OS) for CAD Servers; install server OS upgrades and reinstall OS in event of server failure; review system logs and security logs; maintain server scripts; test disaster recovery; develop, maintain, and provide workstations and MDCs with approved system images.	
BFCA-2	Business Function/CAD Administration	The CAD System Administration shall ensure appropriate security and user permissions, by agency and sub-group, are identified and applied to the CAD system environment.	
BFCA-3	Business Function/CAD Administration	The CAD System Administration shall test, install, and upgrade CAD antivirus releases and patches.	
BFCA-4	Business Function/CAD Administration	The CAD System Administration service shall perform routine server maintenance tasks and ensure proper backups of system volumes.	
BFCA-5	Business Function/CAD Administration	The service shall provide Geo-file Maintenance. Since the geo-file is the basis for many CAD system decisions and functions, it is critical that the geo-file is continuously monitored and updated on a timely basis.	
BFCA-6	Business Function/CAD Administration	The CAD system's geo-file shall be updated to reflect changing conditions, to include: new street constructions; response agency boundary realignments; new site/structure construction; changes in descriptive (i.e., attribute) information stored in the geo-file, including changes in attributes (e.g., street and landmark names, boundary IDs, address ranges of Road Center Line [RCL] segments).	
BFCA-7	Business Function/CAD Administration	The CAD System Administration shall provide for Security to prevent unauthorized access to system modules and data.	
BFCA-8	Business Function/CAD Administration	The CAD System Administration Security Sample Requirements, to include: employing data security measures that are compliant with applicable State and Federal security standards; and employing data encryption that meets Criminal Justice Information Services (CJIS) security policy standards for any exchange or transmittal of CAD data between remote devices and CAD system servers.	
BFCA-9	Business Function/CAD Administration	The CAD System Administration Security shall provide a security profile to control individual user access to the various modules, applications, functions, features, and data available within the CAD system.	

BFCA-10	Business Function/CAD Administration	The CAD System Administration Security shall provide security to ensure that Fire and EMS personnel do not have access to law enforcement incidents when CJIS data is restricted to only law enforcement user access.	
BFCA-11	Business Function/CAD Administration	The CAD System Administration Security shall meet all DoD CS requirements.	
BFCA-12	Business Function/CAD Administration	The CAD System Administration Security shall be capable of using biometric identification (e.g., thumb print identification, retinal ID) to control system access and privileges.	
BFCA-13	Business Function/CAD Administration	The CAD System Administration Security shall provide a "single entry" to enable logons to multiple authorized systems available through the system.	
BFCA-14	Business Function/CAD Administration	The CAD System Administration Security shall limit access to system functions and data by physical device (e.g., PCs, terminals), as well as by user ID.	
BFCA-15	Business Function/CAD Administration	The CAD System Administration Security shall have the capability to automatically log-off CAD workstations based on inactivity periods set by the system administrator for specific user groups, users, and workstations.	
BFCA-16	Business Function/CAD Administration	The CAD System Administration Security shall provide the ability to "lock out" a user after a system administrator-defined number of failed attempted logons.	
BFCA-17	Business Function/CAD Administration	The CAD System Administration Security shall require users to change their individual password after the administrator configurable time limit for use of the same password expires, or for a set time period (e.g., 90 days).	
BFCA-18	Business Function/CAD Administration	The CAD System Administration Security shall provide the ability for individual system users to change their passwords.	
BFCA-19	Business Function/CAD Administration	The CAD System Administration Security shall provide the capability for an individual username change (e.g., getting married) and shall keep a link to historical data.	
BFCA-20	Business Function/CAD Administration	The service shall provide for Logging. In order to be able to meet post-incident analysis and legal requirements, all CAD transactions shall be logged in the system's transaction audit database.	
BFCA-21	Business Function/CAD Administration	The service shall provide a CAD transaction audit database with all stored transactions completed on open/active incidents, to include: the transaction's date and time stamp; the user and workstation ID performing the transaction; and the before and after results of the transaction.	
BFCA-22	Business Function/CAD Administration	The service shall capture transaction information associated with all CAD Security transactions—including any time a CAD user views, prints, edits, adds, or deletes the Security information within the CAD system.	

BFCA-23	Business Function/CAD Administration	The service shall store the date, time, workstation ID, and user ID associated with unsuccessful sign-on attempts.	
BFCA-24	Business Function/CAD Administration	The service shall provide Configuration parameters that enable it to be tailored to meet the requirements of the agencies using it, rather than having to be customized to meet those requirements.	
BFCA-25	Business Function/CAD Administration	The service shall establish the types of agencies and their unique parameters (e.g., fire, law enforcement, EMS, fire and EMS) that shall be included in the system.	
BFCA-26	Business Function/CAD Administration	The service shall enable authorized system administrators to create and modify CAD configuration parameters to meet agency requirements.	
BFCA-27	Business Function/CAD Administration	The service shall enable authorized system administrators to modify CAD configuration parameters without support from the manufacturer of the system.	
BFCA-28	Business Function/CAD Administration	The service shall include functionality for an interactive, menu-driven, GUI-based tool that allows authorized administrators to easily update and modify parameters.	
BFCA-29	Business Function/CAD Administration	The service shall provide Table Maintenance to maintain all CAD functions and operations in tables that can be changed by the agency.	
BFCA-30	Business Function/CAD Administration	The service shall include CAD tables that are maintained using entry windows.	
BFCA-31	Business Function/CAD Administration	The service shall include CAD Table Maintenance entry windows that have context-sensitive, field-level help.	
BFCA-32	Business Function/CAD Administration	The service shall enable changes made to CAD tables to become immediately effective and shall not affect overall system availability, nor require any system down time.	
BFCA-33	Business Function/CAD Administration	The service shall provide Communication Center / PSAP Relocation to account for replacement, or movement, of any existing equipment including base computers, terminals, network, and personnel.	
BFCA-34	Business Function/CAD Administration	The service shall account for coordination of external inputs to the CAD system from third-party vendors (e.g., telephone, data, 9-1-1) for a minimal loss of functionality.	
BFCA-35	Business Function/CAD Administration	The service shall provide for CAD Catch-Up, which is the ability to recover missed information due to the interruption of CAD services. This allows the agency to enter activity data performed during the interruption of service (e.g., a hardware failure of the CAD system causes the entire system to be inoperable).	

Appendix D17 – System Functions

Requirement ID	Category	Requirement	Threshold/Objective
SF-1	System Functions	The service shall provide System Functions, enabling the system administrator to define the rules for automatic CFS event notifications.	
SF-2	System Functions	The service shall provide the ability to create messages that are retained in the system and sent at pre-specified times.	
SF-3	System Functions	The service shall provide the ability to maintain a log of all messages processed by the system.	
SF-4	System Functions	The service shall allow the user to send and store messages to other users, groups, positions, or mobile devices.	
SF-5	System Functions	The service shall provide the ability to create and maintain automatic reminders of scheduled activities (e.g., radio tests).	
SF-6	System Functions	The service shall provide Contact List, allowing the creation, search, and maintenance of contacts and their information.	
SF-7	System Functions	The service shall provide for Premises Information / Hazards. This capability allows for the CAD system to appropriately provide information specific to a particular location or premises (e.g., hazardous or flammable chemicals, has outstanding warrant, history of violence, aggressive dogs on site, list of Critical Infrastructure/Key Resources).	
SF-8	System Functions	The service shall provide Communications Center / PSAP Standard Operating Procedures (SOPs).	
SF-9	System Functions	The service shall provide the ability to store and easily retrieve SOPs for the PSAP.	
SF-10	System Functions	The service shall provide a SOP tool to prompt the user to ask for additional information, perform certain tasks, or relay critical information to responding units or other responders.	
SF-11	System Functions	The service shall provide Agency-Specific Incident / Location / Unit SOPs.	
SF-12	System Functions	The service shall be able to store SOPs associated with incident types, properties, and/or units.	
SF-13	System Functions	The service shall make SOPs available for viewing and/or transmitting when: an associated incident type is encountered; the response is to a specific location with unique response/operational requirements; and/or specialized units are assigned to the incident.	
SF-14	System Functions	The service shall include optional, more sophisticated functionality (e.g., alert and check off of tasks, notifications made, etc.).	

SF-15	System Functions	The service shall provide Remote Access by users outside of the communications center. Access includes permission-based views of CAD system data by certain workstations and/or individuals. Remote access shall include security-controlled, web-based access.	
SF-16	System Functions	The service shall provide CAD Workstation-to-CAD Workstation Messaging from one CAD workstation to another.	
SF-17	System Functions	The service shall enable the system administrator to disable the Messaging function, if desired on an agency basis.	
SF-18	System Functions	The service shall provide Incident Command Support to provide data to support National Incident Management System (NIMS)-required reporting from an RMS.	
SF-19	System Functions	The service shall provide the ability to track roles, tasks, and situation reports.	
SF-20	System Functions	The service shall provide NIMS functions directly or through an interface with an external system.	
SF-21	System Functions	The service shall interface to [*insert specific application/product*] incident command software.	
SF-22	System Functions	The service shall provide Narrative Field “Shorthand”/ Auto Text by recognizing character patterns and automatically filling in expanded text. For example, a dispatcher enters ‘PPE’ in a field and the text expands to indicate that ‘Personal Protective Equipment’ is required on an incident.	
SF-23	System Functions	The service shall provide the capability of Command Line / GUI. The CAD system shall include the ability to be operated via a command line entry using mouse and keyboard, or both.	
SF-24	System Functions	The service shall provide Date/Time Stamps to log CAD activities, to include: status changes; task accomplishments (i.e., Fire Attack Initiated, Time Fire Declared Under Control, Time at Patient); and notifications, as well as many other system transactions and the time they occur.	
SF-25	System Functions	The service shall provide a Unit Status Transitions Matrix in order to prohibit unit status transitions that do not conform to the business rules of the agency.	
SF-26	System Functions	The service shall have a Single Sign-on for CAD and CAD subsystems.	
SF-27	System Functions	The service shall have a Multi-Agency / Multi-Jurisdictional Capability to seamlessly create multiple independent and linked incidents for each agency or jurisdiction associated to the incident, without duplicating any data-entry.	

Appendix D18 – Reporting and Monitoring

Requirement ID	Category	Requirement	Threshold/Objective
RM-1	Reporting and Monitoring	The service shall have the capability to manage the workflow of the call takers and dispatchers, including training and testing functions.	
RM-2	Reporting and Monitoring	The service shall provide Dispatch Supervisor Support with the ability for a supervisor, or another dispatcher with appropriate system permissions, to observe the activity (e.g., pending events queue, active events, available units list, map) of a given dispatcher.	
RM-3	Reporting and Monitoring	The service shall have a CAD Management Reporting System to provide standard reports that can be run using a variety of flexible parameters. New reports shall be defined, either through the CAD system or a third-party reporting tool, and shall then be stored as a standard report available through the CAD system.	
RM-4	Reporting and Monitoring	The service shall provide for Training and Testing and shall clearly be identified as the training environment (e.g., "TRAINING" prominently displayed on the screen).	
RM-5	Reporting and Monitoring	The service shall have a separate Enhanced 9-1-1 (E911) test connection or information (i.e., wireline, cellular, no record found, VoIP), and shall provide realistic training regarding incoming E911 data.	
RM-6	Reporting and Monitoring	The service shall provide for Snapshot / Incident Replay to provide a detailed, system-wide snapshot report—and/or graphic display—of the system status. This shall include all units and events, based on a user-specified date and time, as well as an incident replay based on a user-specified date and time, specific incidents, or other CAD events.	

Appendix D19 – Interfaces

Requirement ID	Category	Requirement	Threshold/Objective
INT-1	Interfaces	The service shall provide Interfaces by which the CAD system communicates information with other systems within the PSAP—such as E911 systems—or with external systems—such as federal databases, fire toning systems, or Emergency Operations Centers (EOCs).	
INT-2	Interfaces	The CAD system interface shall provide connectivity most commonly through using TCP/IP protocols—although some legacy systems also use asynchronous serial connections, and other forms of direct-connect methods—to transfer data between the external system and the CAD system.	
INT-3	Interfaces	The service shall provide Essential Interface of an E911 interface that imports subscriber information (i.e., ANI and ALI) for each E911 caller—as provided by the telephone company—into CAD-compliant entry process.	
INT-4	Interfaces	The service shall provide Essential Interface Query to External Databases (i.e., Federal, State, NCIC, local). Queries to the State, local, RMS, and National databases shall automatically occur from selected CAD commands using the messaging system interface.	
INT-5	Interfaces	The service shall provide Essential Interface to Messaging Subsystems (i.e., radio, paging/toning, email, text messaging), providing the ability to communicate with external messaging subsystems. This is one of the most important interfaces in terms of situational awareness and officer safety.	
INT-6	Interfaces	The service shall provide Essential Interface to Records Management Systems. Ideally, the RMS shall have a robust interface, designed to work in conjunction with the CAD application, to enable a higher level of information sharing and workflow capabilities.	
INT-7	Interfaces	The service shall provide Additional Interfaces. It is often desirable to have a direct interface between the CAD system and other key law enforcement systems (e.g., other CAD systems in the area, alarm systems, MDCs).	
INT-8	Interfaces	The service shall provide CAD-to-CAD functionality, which typically allows a single CAD system to interface to one or more CAD systems.	
INT-9	Interfaces	The service shall provide Essential Interface for MDCs, which provides an extension to the CAD dispatch services from law enforcement vehicles, fire department rigs, and ambulances. Law enforcement will require forms and functions to enable the querying of external databases. Fire rigs will require the ability to access pre-plan data and information. Ambulance crews will require forms and functions related to the management of patient data and medical procedures.	

INT-10	Interfaces	The service shall provide Essential Interfaces for Locational Systems Interfaces, which is an automated access to address, geographic, and mapping information for public safety agencies. The primary locational systems include Automatic Vehicle Location (AVL), GIS, mobile and real-time mapping, and device mapping. These systems provide historic data that can be used in geospatial and temporal analytics.	
INT-11	Interfaces	The service shall provide for Administration Interfaces.	
INT-12	Interfaces	The service shall have the ability to import and display the radio ID—and optionally the officer ID—information to the dispatcher by those keying mobile and/or portable radios.	
INT-13	Interfaces	The service shall have the ability to interface and synchronize all servers and CAD workstations with the master time clock.	
INT-14	Interfaces	The service shall provide the ability for the agency to schedule personnel, including communications center personnel and officers.	
INT-15	Interfaces	The service shall provide Communications Interfaces. There are several communications-based interfaces that allow CAD-generated information to be transmitted to others via email, messaging, and the Internet. The CAD system shall accept, depending on agency policy, non-dispatchable incidents across the Internet.	
INT-16	Interfaces	The service shall take into account that Incidents accepted across the Internet will be of a general nature, in which a case (i.e., report) number may be needed for insurance purposes. The case number shall be generated and recorded. The incident shall be recorded in the incidents/events history database for statistical reporting.	
INT-17	Interfaces	The service shall provide for pages or text messages to be sent to pre-defined recipients or groups of recipients based on event type.	
INT-18	Interfaces	The service shall provide the capability for a CAD operator (e.g., PSAP personnel or CAD users) to page, email, or text a message to pre-defined recipients or groups of recipients.	
INT-19	Interfaces	The service shall provide Integration / Interfaces with Other Systems.	
INT-20	Interfaces	The service shall allow the agency direct access to the underlying system information stored in the database (e.g., Open Database Connectivity [ODBC], File Transfer Protocol [FTP], web services) for future interface configuration, as well as appropriate database and system documentation to support this access.	
INT-21	Interfaces	The service shall provide a capability to flag a CAD call for submission as a Suspicious Activity, and submit that call to the agency's intelligence/counterterrorism unit or designated Fusion Center.	
INT-22	Interfaces	The service shall provide an interface to [*insert specific application/product here*] incident command software.	
INT-23	Interfaces	The service shall provide an interface to [insert specific application/product here] records management software.	

INT-24	Interfaces	The service shall provide an interface with alarm monitoring companies using Automated Secure Alarm Protocol (ASAP). This interface shall conform to standards contained in the Association of Public-Safety Communications Officials (APCO)/Central Station Alarm Association (CSAA) ANS 2.101.1-2008: Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) External Alarm Interface Exchange [10].	
INT-25	Interfaces	The service shall provide Nationwide Suspicious Activity Reporting (SAR) Initiative Functionality, which is designed to support the sharing of information about suspicious activity, incidents, or behavior—hereafter, collectively referred to as suspicious activity or activities—that have a potential terrorism nexus.	
INT-26	Interfaces	The service shall include State and major urban area Fusion Centers, and their law enforcement, homeland security, or other information sharing partners at the Federal, State, local, and tribal levels to the fullest extent permitted by law.	
INT-27	Interfaces	The service shall allow users to flag a CFS as "suspicious" with regard to the National SAR Initiative.	
INT-28	Interfaces	The service shall send a "suspicious-flagged" CFS to an external application, database, or Law Enforcement Records Management System (LERMS) that handles SAR reporting.	
INT-29	Interfaces	The service shall provide the capability to notify an intelligence unit/counterterrorism unit when a SAR is submitted.	
INT-30	Interfaces	The service shall provide an EOC Interface.	
INT-31	Interfaces	The EOC Interface service shall have an EOC viewable setting, which can be initiated through a web viewer or license, to allow the EOC to view incidents and units specific to the emergency event.	
INT-32	Interfaces	The EOC Interface service shall allow for incident creation that is within the area of the incident, but be limited to certain incident types, depending on the type of disaster.	
INT-33	Interfaces	The EOC Interface service shall interface to [*insert specific application/product]* incident command software.	
INT-34	Interfaces	The EOC Interface service shall allow for the allocation of certain apparatus/units that can be managed and dispatched out of EOCs for a specific CFS—planned or unplanned—without negatively impacting the CAD system. It is also preferred, in this instance, that activities are manual (i.e., the system shall keep track of all apparatus and personnel for both the agency-wide response and the EOC response area).	
INT-35	Interfaces	The service shall operate IAW the National Emergency Number Association (NENA) i3 Standard for Next Generation 9-1-1 (NG911) GIS Data Model [11].	

INT-36	Interfaces	The service shall support information sharing via a National Information Exchange Model (NIEM)-compliant XML-based schema, as prescribed by the Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA), and IAW DoD Issuance (DoDI) 8320.07 [12].	

Appendix D20 – Common Operational Picture (COP)

Requirement ID	Category	Requirement	Threshold/Objective
COP-1	Common Operational Picture	The system shall enable Common Operational Picture (COP) tools to provide a single, identical display of relevant information across multiple command levels. COP improves situational awareness, thereby fostering effective decision making, rapid staff actions, and appropriate incident execution.	
COP-2	Common Operational Picture	The COP system shall aid with collecting, sharing, and displaying multi-dimensional information that facilitates collaborative planning and distributed responses to complex incidents.	
COP-3	Common Operational Picture	The COP system shall provide consistent, timely, and accurate reporting of critical information for events of local, regional, and National significance.	
COP-4	Common Operational Picture	The COP system shall support auto-ingestion of data from multiple sources.	
COP-5	Common Operational Picture	The COP system shall support interaction with a consolidated, centralized data repository.	
COP-6	Common Operational Picture	The COP system shall be browser-based.	
COP-7	Common Operational Picture	The COP system shall accept interfaces from internal and external authoritative sources (i.e., National Weather Service [NWS]).	

Appendix D21 – GIS/CAD Mapping Integration

Requirement ID	Category	Requirement	Threshold/Objective
MI-1	GIS/CAD Mapping Integration	XXX	

Appendix D22 – 911 Telephony Integration and Data Standards

Requirement ID	Category	Requirement	Threshold/Objective
TIDS-1	9-1-1 Telephony Integration and Data Standards	XXX	

Appendix D23 – References

[1] https://uscode.house.gov/view.xhtml?path=/prelim@title5/title5a/node20&edition=prelim.

[2] https://tools.ietf.org/html/rfc3261.

[3] https://tools.ietf.org/html/rfc5060.

[4] https://tools.ietf.org/html/rfc5061.

[5] https://tools.ietf.org/html/rfc4346.

[6] https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

[7] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[8] https://tools.ietf.org/html/rfc3275.

[9] http://xml.coverpages.org/SPMLv2-OS.pdf.

[10] https://www.apcointl.org/images/pdf/Automated%20Secure%20Alarm%20Protocol.pdf.

[11] https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-006.1.1-2020_ng9-1-.pdf.

[12] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/832007p.pdf.

Appendix D24 – Acronyms and Definitions

AES	Advanced Encryption Standard
ALI	Automatic Location Identification
ALS	Advanced Life Support
ANI	Automatic Number Identification
APCO	Association of Public-Safety Communications Officials
ASAP	Automated Secure Alarm Protocol
ATC	Authority to Connect
ATO	Authority to Operate
AVL	Automatic Vehicle Location
BCF	Border Control Function
BLS	Basic Life Support
BOLO	Be-on-the-Look-Out
CAD	Computer-Aided Dispatch
CFS	Call for Service
CJIS	Criminal Justice Information Services
COP	Common Operational Picture
CS	Cybersecurity
CSAA	Central Station Alarm Association
DHS	Department of Homeland Security
DoD	Department of Defense
DoDI	Department of Defense Issuance
DoS	Denial-of-Service
E911	Enhanced 9-1-1
ECRF	Emergency Call Routing Function
EMT	Emergency Medical Technician
EOC	Emergency Operations Center
ESInet	Emergency Services Internet Protocol Network
ESRP	Emergency Services Routing Proxy
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FRD	Functional Requirements Document
FTP	File Transfer Protocol
HIPAA	Health Information Portability and Accountability Act
GUI	Graphical User Interface
GUID	Globally Unique Identifier
IAW	In Accordance With
IG	Inspector General
IMS	IP Multimedia Subsystem
JITC	Joint Interoperability Test Command
LbyR	Location-by-Reference
LbyV	Location-by-Value
LDAP	Lightweight Directory Access Protocol
LERMS	Law Enforcement Records Management System
LIS	Location Information Server
LoST	Location-to-Service Translation
MCI	Mass Casualty Incident
MDC	Mobile Data Computer
MEP	Method Exchange Pattern
MOU	Memorandum of Understanding
NENA	National Emergency Number Association
NG911	Next Generation 9-1-1
NIEM	National Information Exchange Model

NIMS	National Incident Management System
NWS	National Weather Service
ODBC	Open Database Connectivity
OIG	Office of Inspector General
OS	Operating System
PA	Public Address
PCR	Patient Care Report
PFPA	Pentagon Force Protection Agency
PKI	Public Key Infrastructure
PRF	Policy Routing Function
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RCL	Road Center Line
RMS	Records Management System
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Protocol
SAML	Security Assertion Markup Language
SAR	Suspicious Activity Reporting
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIPS	Secure Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNPP	Simple Network Paging Protocol
SOP	Standard Operating Procedure
SPML	Service Provisioning Markup Language
SWAT	Special Weapons and Tactics
TAP	Telocator Alphanumeric Protocol
TCP	Transport Control Protocol
TDM	Time-Division Multiplex
TLS	Transport Layer Security
UDP	User Dataram Protocol
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol
WCTP	Wireless communications Transfer Protocol
WMD	Weapon of Mass Destruction
XACML	Extensible Access Control Markup Language