DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY, REFER TO: Joint Interoperability Test Command (JTE) **14 Apr 15**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Spōk Enterprise Alert Release 11.11.0.286

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Errata 1," 1 July 2013
(c) and (d), see Enclosure 1

1. **Certification Authority.** Reference (a) establishes the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for UC products.

2. **Conditions of Certification.** The Spōk Enterprise Alert Release 11.11.0.286; hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (b), and is certified for joint use on the Defense Information Systems Network (DISN) as an enhanced emergency service (E911) Management System without any conditions (see Table 1). The SUT was tested and certified with the CS1000M Small End Office (SMEO) or Private Branch Exchange (PBX), release Succession Defense Switched Network (DSN) 5.0, and the Avaya Aura Communication Manager (CM) Local Session Controller (LSC), release 6.3.6 with Patch 03.0.124.0-21862 configured with Avaya Enablement (AE) Services, release 6.3.3. The certified interfaces for each of these switches are specified in Table 2. The SUT is certified for joint use with any digital switching system or Session Controller that is functionally identical to the CS1000M or Avaya Aura CM configured with Avaya AE Services and is or was on the UC Approved Products List (APL). This certification expires upon changes that affect interoperability, but no later than three years from the date of the UC APL memorandum.

Table 1. Conditions

Condition	Operational Impact	Remarks
Not applicable; the Spōk Enterprise Alert Release 11.11.0.286 meets all of the Unified Capabilities Requirements, Reference (c) joint critical interoperability requirements.		

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status and Table 3 provides the Capability Requirements (CR) and Functional Requirements (FR) status. Table 4 provides a UC APL product summary.

Table 2. SUT Interface Status

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks
Session Controller and Legacy Switch Interfaces			
ISDN T1 PRI NI2 (C)	1 (See note 2.)	Met	The SUT met the critical CRs and FRs for this interface.
Analog (C)	1 (See note 2.)	Met	The SUT met the critical CRs and FRs for this interface, which is used solely for passive call monitoring.
IP (C)	1	Not Tested	The SUT does not support this interface.
SUT Management Interface			
Serial EIA-232 (C)	1	Not Tested	The SUT does not support this interface.
IP (C)	1 (See note 3.)	Met	The SUT met the critical CRs and FRs for this interface.

NOTES:
1. The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3.
2. The SUT was tested with the CS1000M, release Succession DSN 5.0, and the Avaya Aura CM, release 6.3.6 with Patch 03.0.124.0-21862 configured with Avaya AE Services, with the Avaya CS2100, release Succession Enterprise 09.1. The SUT is certified for joint use with any digital switching system or Session Controller that is or was previously on the UC APL certified with ISDN T1 PRI NI2 and analog interfaces and is functionally identical to the CS1000M, Avaya Aura CM configured with Avaya AE Services.
3. The IP interface was for Operation, Administration, Maintenance, and Provisioning (OAM&P) traffic for SUT management and connectivity to the Avaya AE Services. The Avaya AE Services is required for the Avaya Aura CM Session Controller. This allows the SUT to forward calls to End Instruments that do not have a non-Direct Inward Dial number.

LEGEND:

AE	Application Enablement	IP	Internet Protocol
APL	Approved Products List	ISDN	Integrated Services Digital Network
C	Conditional	NI2	National ISDN Standard 2
CR	Capability Requirements	PRI	Primary Rate Interface
CM	Communication Manager	SUT	System Under Test
DSN	Defense Switched Network	T1	Digital Transmission Link Level 1
EIA	Electronic Industries Alliance	UC	Unified Capabilities
FR	Functional Requirements	UCR	Unified Capability Requirements
ID	Identification		

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	E911 Management System Requirements (R)	3.6	Met (See note 2.)

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. Security testing is accomplished by DISA-led Information Assurance test teams and the results are published in a separate report, Reference (d).

LEGEND:

CR	Capability Requirement	ID	Identification
DISA	Defense Information Systems Agency	R	Required
E911	enhanced emergency service	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements

Table 4. UC APL Product Summary

Product Identification			
Product Name	Spōk Enterprise Alert		
Software Release	11.11.0.286		
UC Product Type(s)	E911 Management Systems		
Product Description	Enhanced emergency service (E911) Management System		
Product Components (See note.)	**Component Name**	**Version**	**Remarks**
Application/Database Server	Enterprise Alert Server Dell PE R720	Enterprise Alert 11.11.0.286	
		EADM Version11.11-Build:25	
		MS Windows 2012 Server R2 SP2	
		MS SQL 2012	
		XnAlert – Version 11.11.0.286	
		EAFFTmr version 11.11.0.286	
		Genbridge version 11.0.0.220	
		genCiscoMon version 11.0.0.10	
		FW1-Form Version 11.11.0.286	
		xnGetTMS Version 11.11.0.272	
		xnupdate Version 11.11.0.272	
		XnSentry version 11.11.0.286	
		XnIntradoFTP version 11.0.0.0	
		WindStreamFtp version 11.0.0.0	
		FilePurge version 11.11.0.374	
		Purge911 version 11.11.0.374	
		Amcom_aes_service version 5.5.0.0	
		AlwaysUP version 9.0.3.81	
Management Server	Management Server Dell PE R310	11.11-Build:25	
		MS Windows 2008 Server R2 SP2	
		EADM Version 11.11-Build:25	
Bypass box	Bypass box	Not Applicable	
Sentry Client Workstation	Spōk Sentry Workstation	MS Windows 7 Professional SP1	
		XnSentry version 11.11.0.286	
		XnReport version 11.11.0.272	
		911play version 11.11.0.374	

NOTE: The detailed component and subcomponent list is provided in Enclosure 3.

LEGEND:

APL	Approved Product List	R2	Release 2
E911	enhanced emergency service	SQL	Structured Query Language
EADM	Enterprise Alert Database Management	TDD	Telecommunications Device for the Deaf
MS	Microsoft	UC	Unified Capabilities
pc/psap	personal computer/public safety answering point		

4. **Test Details.** This certification is based on interoperability testing, review of the vendor's Letters of Compliance (LoC), and DISA Certifying Authority (CA) Recommendation for inclusion on the UC APL. Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 9 through 21 March 2015 using test procedures derived from Reference (c). Review of the vendor's LoC was completed on 13 November 2014. Information Assurance testing was conducted by DISA-led Information Assurance test teams and the results are published in a separate report, Reference (d). Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

5. **Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified IP Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at

https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated information is available on the DISA UCCO website located at http://www.disa.mil/Services/Network-Services/UCCO.

6. **Point of Contact (POC).** The JITC point of contact is Ms. Sibylle Gonzales, commercial telephone (520) 538-5483, DSN telephone 879-5483, FAX DSN 879-4347; e-mail address sibylle.j.gonzales.civ@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTE (Ms. Sibylle Gonzales) P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 1424702.

FOR THE COMMANDER:

3 Enclosures a/s

for RIC HARRISON
Chief
Networks/Communications and UC Portfolio

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
USD(AT&L)
ISG Secretariat, DISA, JTA
U.S. Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA (ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division
US Coast Guard, CG-64
DISA/TEMC
DIA, Office of the Acquisition Executive
NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V
HQUSAISEC, AMSEL-IE-IS
UCCO

ADDITIONAL REFERENCES

(c) Joint Interoperability Test Command, “E911 Management Systems Test Procedures for Unified Capabilities Requirements (UCR) 2013," Draft
(d) Joint Interoperability Test Command, “Information Assurance (IA) Assessment Report for Spok Enterprise Alert Database Management (EADM) Release (Rel.) 11.11.0.286 (Tracking Number 1424702),” Draft

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Spōk Enterprise Alert Release 11.11.0.286 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	Headquarters United States Army Information Systems Engineering Command (HQUSAISEC)
Sponsor Point of Contact	Mr. Jordan Silk, USAISEC ELIE-ISE-ES, Building 53301, Fort Huachuca, Arizona 85613, e-mail: jordan.r.silk.civ@mail.mil
Vendor Point of Contact	Erdman, Robert bob.erdman@Spōk.com 800-852-8935
System Name	Spōk Enterprise Alert
Increment and/or Version	11.11.0.286
Product Category	E911 Management Systems
System Background	
Previous certifications	None
Tracking	
UCCO ID	1424702
System Tracking Program ID	5046
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Errata 1, Section 3.6, E911 Management Systems
Remarks	
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona
LEGEND:	
ID Identification UCCO Unified Capabilities Connection Office	

2. SYSTEM DESCRIPTION. Standalone enhanced emergency service (E911) Management Systems are Unified Capabilities (UC) appliances that enable a reliable user location to be provided to emergency response dispatch centers when a 911 call is made from a UC End Instrument (EI). E911 Management Systems are intended to support wireline E911 service, including support for UC subscribers using softphones and subscribers connected via wireless Local Area Network (LAN) interfaces, such as Institute of Electrical and Electronics Engineers (IEEE) 802.11b/g/n.

Spōk's Enterprise Alert system consists of an Enterprise Alert Server, Management Server, bypass box, and Sentry Client Workstation. The purpose of the Enterprise Alert Server is to host the database containing the Automatic Number Identification (ANI) and location information and the interface to extract and communicate the ANI and Automatic Location Identification (ALI) information with a public Public Safety Answering Point (PSAP). The monitor workstation(s) communicate directly with the file/application server for the purpose of retrieving the emergency call identification and location information only.

The SUT is installed on a dedicated server that serves as the primary database server and applications engine. Enterprise Alert™ is a Windows server based application that upon dialing

911 from a Local Session Controller (LSC)/Private Branch Exchange (PBX) station line translates the station Identification (ID) into an associated Direct Inward Dial (DID) number that allows PSAP callbacks and directs emergency response personnel to the exact caller location. Each 911 call from the LSC/PBX passes through the Enterprise Alert™ system to the E911 Tandem for routing and local 911 PSAP call dispatching. The ANI update feature stores and translates the LSC/PBX number from the extension and the Calling Party Identification (CPID) to an assigned DID number. If no DID is assigned to a particular extension, then Enterprise Alert™ translates to the nearest DID location. Enterprise Alert™ integrates with LSC/PBX systems to identify an extension and location of 911 or 9-911 callers. The caller may dial the digits "911" or "9-911" from any internal analog or digital extension on the LSC/PBX and the call will be reported on the local Enterprise Alert™ system. For each call that is received by the Enterprise Alert™ server, an audible alarm is sounded and the monitor is populated with number and location detail regarding the caller. Enterprise Alert™ automatically connects the audio segment of the call from the LSC/PBX to the PSAP.

The SUT Integrated Services Digital Network (ISDN) Digital Transmission Link Level 1 (T1) Primary Rate Interface (PRI) National ISDN 2 (NI2) trunk interface is used to receive the ANI information when a 911 call is made from the phone within a local Session Controller (SC)/Private Branch Exchange (PBX). The PRI trunk is connected to the AudioCodes (SmartWorks DT6409TE PCIe) digital board. The Enterprise Alert module will retrieve ANI and other relevant information from PRI trunk by using SmartWorks Application Programming Interface (APIs). The ANI is then propagated by using a protocol, which is proprietary to Spōk and is comprised of a series of numeric messages and commands that represent the state of the interface and the channels of the device. The analog lines are connected to second AudioCodes 8-port analog board (SmartWorks LD809-eh PCIe) in order to conference a local security team to the 911 call in progress.

The Management Server is a Security Technical Implementation Guide (STIG)-compliant, Common Access Card (CAC)-enabled, Dell Power Edge R320 component with Windows Server 2008 Release 2 (R2) Standard Service Pack (SP) 1 OS platform with the Enterprise Alert web application used to manually add, delete, and change system database records and set user profiles.

The Bypass Box is a hardware appliance that functions as an alarm and "watch dog" device. The Bypass box is capable of detecting issues with PRI connection. Once the issue with PRI connection or software is detected, the bypass box will put the system in "failure" mode so the 911 calls will be sent through without any modification so the call can be answered by public PSAP.

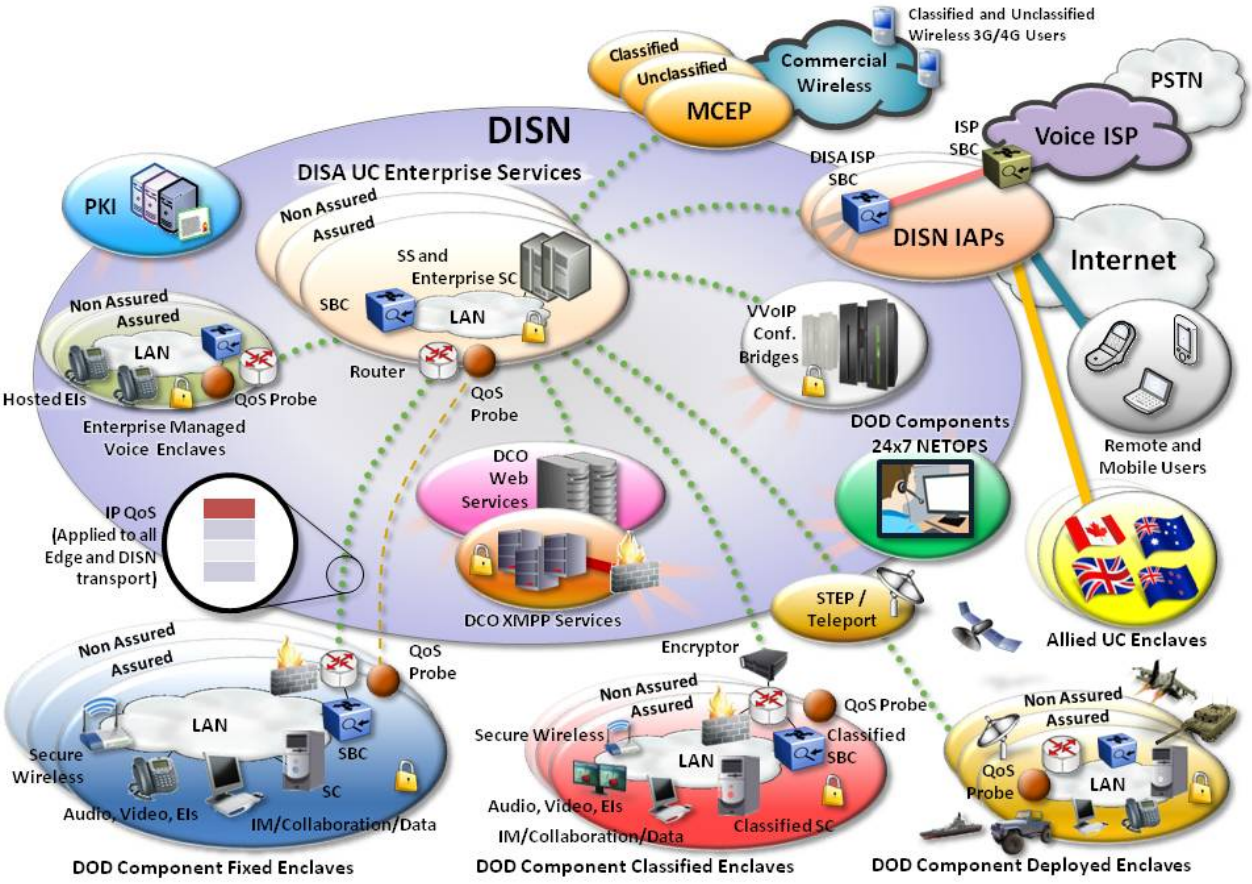
The Spōk Sentry Client Workstation is a STIG-compliant, CAC-enabled, Dell Optiplex XE series personal computer with Windows 7 Professional SP 1 OS platform. Installed on the workstation is the XnSentry application that displays important 911-caller information as soon as the call is received by the main EA system. The status bar on this screen also displays an icon, which represents the main EA system(s) the workstation is connected to.

3. OPERATIONAL ARCHITECTURE. The UC architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and

Service/Agency installation switches. The Department of Defense (DoD) Chief Information Officer (CIO) and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The UC architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational UC architecture in which the SUT may be used and Figure 2-2 the E911 Management System Architecture for UC E911 Services.

4. TEST CONFIGURATION. The test team tested the SUT at Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona in a manner and configuration similar to that of a notional operational environment. Testing of the system's required functions and features was conducted using the test configuration depicted in Figure 2-3. Information Assurance (IA) testing used the same configuration.

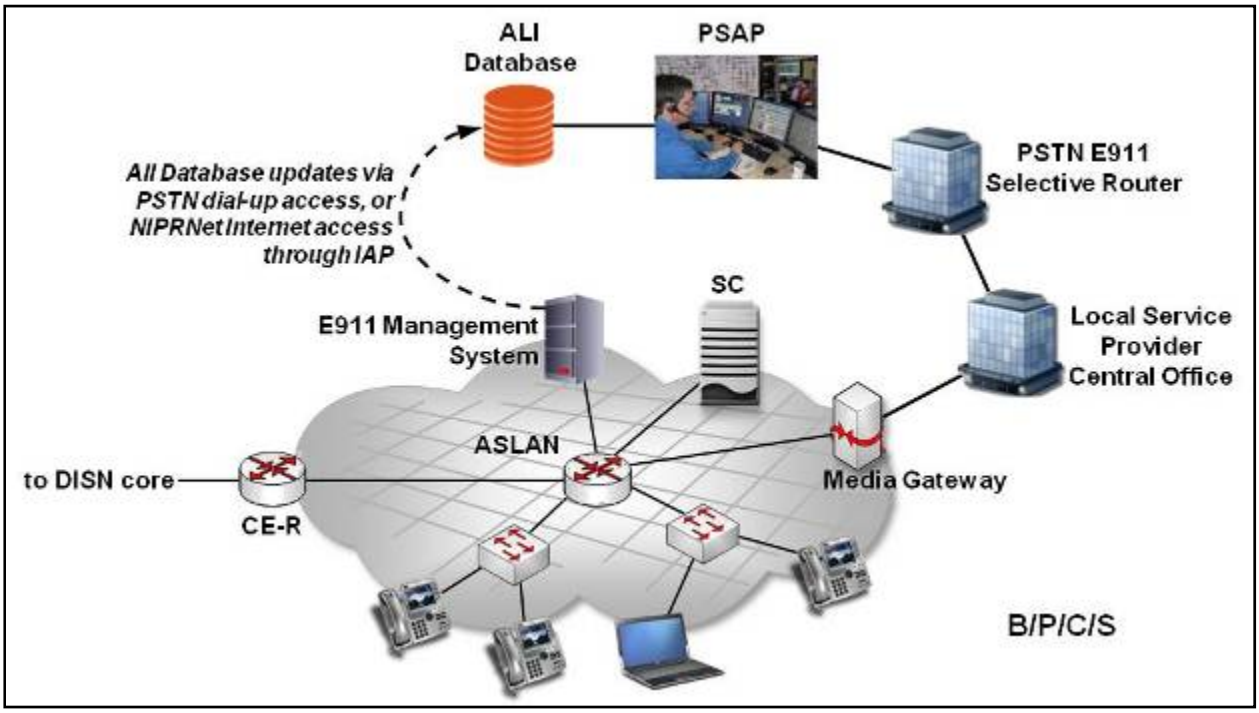
5. METHODOLOGY. Testing was conducted using E911 Management System requirements derived from the Unified Capabilities Requirements (UCR) 2013, Errata 1, Reference (b), and E911 Management System test procedures, Reference (c). Any discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of Defense Information System Agency (DISA) via a vendor Plan of Action and Milestones (POA&M), which will address all new critical Test Discrepancy Reports (TDRs) within 120 days of identification.



LEGEND:

DCO	Defense Connection Online	NETOPS	Network Operations
DISA	Defense Information Systems Agency	PKI	Public Key Infrastructure
DISN	Defense Information Systems Network	PSTN	Public Switched Telephone Network
DoD	Department of Defense	QoS	Quality of Service
EI	End Instrument	SBC	Session Border Controller
IAP	Internet Access Point	SC	Session Controller
IM	Instant Messaging	SS	Softswitch
IP	Internet Protocol	STEP	Standardized Tactical Entry Point
ISP	Internet Service Provider	UC	Unified Capabilities
LAN	Local Area Network	VVoIP	Voice and Video over IP
MCEP	Multi Carrier Entry Point	XMPP	Extensible Messaging and Presence Protocol

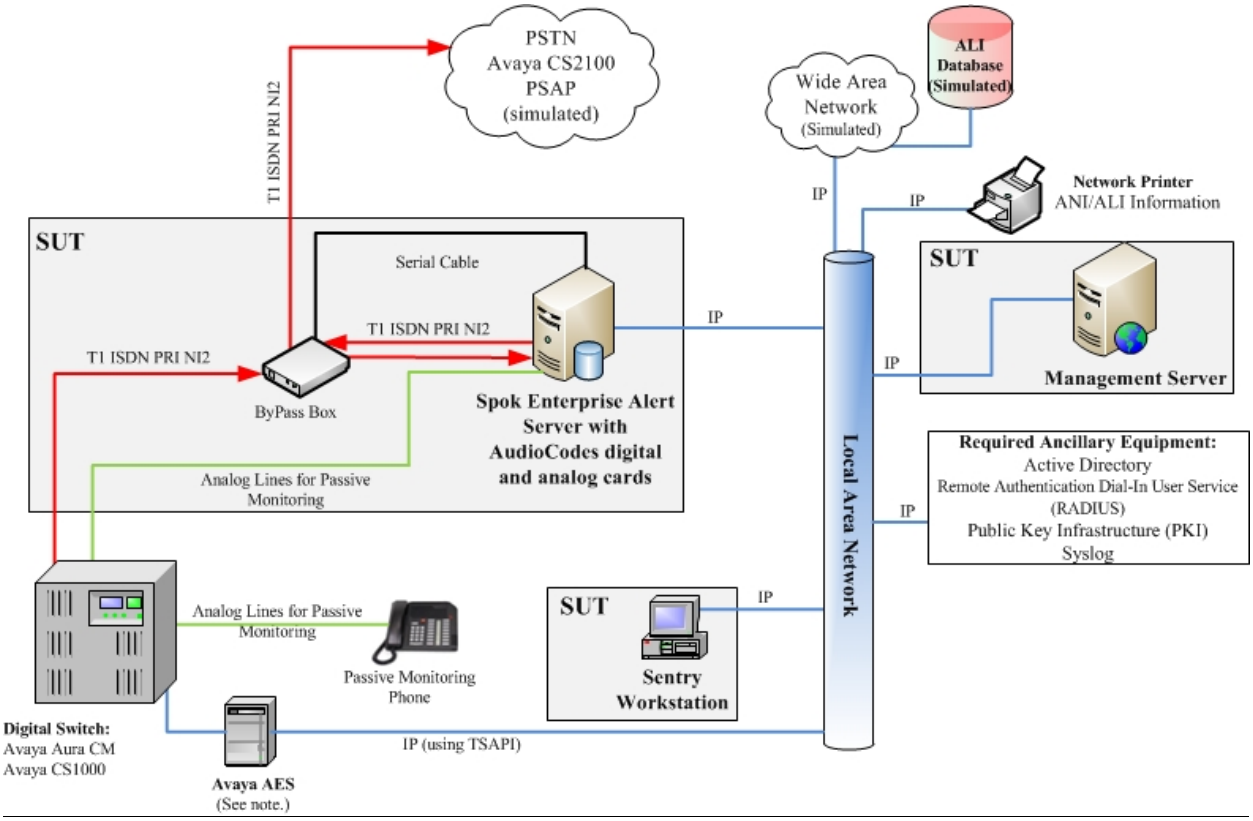
Figure 2-1. Notional UC Network Architecture



LEGEND:

ALI	Automatic Location Identification	NIPRNet	Unclassified-But-Sensitive Internet Protocol Router Network
ASLAN	Assures Services Local Area Network	PSAP	Public Safety Answering Point
B/P/C/S	Base/Post/Camp/Station	PSTN	Public Switched Telephone Network
CE-R	Customer Edge Router	SC	Session Controller
DISN	Defense Information Systems Network	UC	Unified Capabilities
E911	enhanced emergency service		
IAP	Internet Access Point		

Figure 2-2. E911 Management System Architecture for UC E911 Services



NOTE: The Avaya AE Services is required for the Avaya Aura CM Session Controller. This allows the SUT to forward calls to End Instruments that do not have a non-Direct Inward Dial number.

LEGEND:

AE	Application Enablement	NI2	National ISDN Standard 2
ALI	Automatic Location Identification	PRI	Primary Rate Interface
ANI	Automatic Number Identification	PSAP	Public Safety Answering Point
CM	Communication Manager	PSTN	Public Switched Telephone Network
CS	Communication Server	SUT	System Under Test
IP	Internet Protocol	T1	Digital Transmission Link Level 1
ISDN	Integrated Services Digital Network	TSAPI	Telephony Services Application Programming Interface

Figure 2-3. SUT Test Configuration

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The interface, Capability Requirements (CR) and Functional Requirements (FR), and other requirements for E911 Management Systems are established by UCR 2013, Errata 1, sections 3.6 and 5.

a. Interface Status. The status of JITC interface testing on the SUT is provided in Table 3-1. The UCR 2013, Errata 1, section 3.6.2 states that the E911 Management System shall support signaling interfaces to UC SC products from at least two different vendors, and shall use these interfaces for signaling with those SCs. The UCR 2013, Errata 1 includes the following basic 911 requirements. The emergency services network that handles DoD and PSTN 911 calls may be Time Division Multiplex (TDM)- or Internet Protocol (IP)-based. The E911 Management System may also support one or more proprietary or standardized signaling interfaces to UC SC products. The SC and Softswitch (SS) may support 911 services for Voice over IP (VoIP) and

TDM lines. When the local switching system is in an area with E911 served through a tandem switch, the emergency call is advanced to the tandem switch with calling line ANI or Calling Number Delivery (CND). The SUT met the interface requirements with testing using the ISDN T1 PRI NI2 interface. The SUT also supports an analog interface solely for passive monitoring.

b. Capability and Functional Requirements and Status

(1) The UCR 2013, section 3.6.2 includes the general E911 Management System requirements in the subparagraphs below.

(a) The E911 Management System shall support signaling interfaces to UC SC products from at least two different vendors, and shall use these interfaces for signaling with those SCs. The SUT met the interface requirements with testing the Avaya CS1000M, the Avaya Aura Communication Manager and the Avaya Application Enablement Services using the ISDN T1 PRI NI2 interface.

(b) If the UC SC product supports one or more proprietary signaling interface for E911 Management System interconnection, then the E911 Management System shall support at least one of these interfaces, per the SC vendor's proprietary interface specifications. The SUT does not support this conditional requirement.

(c) If the UC SC product supports one or more standardized signaling interface for E911 Management System interconnection, then the E911 Management System shall support at least one of these interfaces, per standardized interface specifications identified by the SC vendor. The SUT met this requirement with testing for the following Telcordia standards: SR-NWT-002120 and TR-NWT-001268.

(2) The UCR 2013, section 3.6.3 includes the Automatic Location Identification (ALI) Information requirements in the subparagraphs below.

(a) The E911 Management System shall maintain, for each SC to which it interfaces, an appropriate set of location data and corresponding Emergency Location Identification Number (ELINs) that identify the physical locations of each of the EIs served by the SC. The SUT met this requirement with testing.

(b) The E911 Management System shall also maintain any additional data items required by the ALI databases supporting the PSAPs serving the Base/Post/Camp/Station (B/P/C/S) or enclave. These PSAPs are responsible for handling 911 calls from the EIs served by the SCs to which the E911 Management System interfaces. The SUT met this requirement with testing.

(c) The E911 Management System shall be capable of exporting, to a file, ALI data in .csv or National Emergency Number Association (NENA), Version 2.0 or later, formats. The SUT met this requirement with testing.

(d) If the B/P/C/S or enclave requires that ALI data be provided in a proprietary format, then the E911 Management System shall be capable of exporting, to a file, the ALI data in the required proprietary format. The SUT does not support this conditional requirement.

(e) If the E911 Management System supports direct, secure electronic transfer of ALI data to a target ALI database (or to an intermediary application or service that in turn updates the ALI database), and the B/P/C/S or enclave supports and allows such a transfer, then a direct electronic export of ALI data shall be allowed in lieu of exporting the data to a file. The SUT met this requirement with testing.

(f) The E911 Management System shall be capable of exporting ALI data in the circumstances listed in the subparagraphs below. The SUT met this requirement with testing.

1. On a periodic, scheduled basis.

2. In response to a configurable event (i.e., the creation of a new Emergency Response Location [ERL] and ELIN in the system).

3. In response to an administrator's request, on an ad hoc basis.

(3) The UCR 2013, section 3.6.4 includes the End Instrument Location at Registration requirements in the subparagraphs below.

(a) If the SC provides notification of EI registrations, then the E911 Management System shall do all of the following when notified of an EI registration. The SMEO and SC in the test architecture did not provide notification of registration. Therefore, it was not tested.

1. Determine the physical location of the EI, based on IP address assigned to the EI and any additional information provided by the SC at registration notification.

2. Determine the ERL assigned to that location.

3. Keep an internal record of the EI registration that includes the ELIN for the ERL assigned to the EI's location.

4. Acknowledge receipt of the registration notification to the SC, and include the EI's ELIN in that acknowledgement.

(b) If the EI directly provides notification of registration, then the E911 Management System shall do all of the following when notified of an EI registration. The SMEO and SC EIs in the test architecture did not provide notification of registration. Therefore, it was not tested.

1. Determine the physical location of the EI, based on IP address assigned to the EI and any additional information provided by the EI at registration notification.

2. Determine the ERL assigned to that location.

3. Keep an internal record of the EI registration that includes the ELIN for the ERL assigned to the EI's location.

(c) When the E911 Management System is unable to determine the location of a registered EI, it shall perform the configured default behavior for this circumstance. The SUT met this requirement with testing.

(4) The UCR 2013, section 3.6.5 includes the Support for ELIN Query at 911 Call requirements. When queried by an SC processing a 911 call from a registered EI, the E911 Management System shall provide the SC with the ELIN associated with that EI in its internal record. The SUT met this requirement with testing via the ISDN T1 PRI NI2 interface.

(5) The UCR 2013, section 3.6.6 includes the SC Interfaces with E911 Management Systems requirements. SCs are not required to support interfaces to standalone E911 Management Systems. The burden is on the E911 solution to interface to the SC. However, if an SC does support interfaces to E911 Management Systems, then the requirements in this section apply to the SC. Furthermore, the requirements in this section apply only to SCs that are connected to an active E911 Management System. The requirements in this section do not apply to an E911 Management System. Therefore, the requirements in this section were not tested. . However, the SUT met the interface requirements with testing and the vendor's LoC for the ISDN T1 PRI NI2 interface while connected to the Avaya CS2100 Multifunction Switch, Avaya CS1000M Small End Office, and Avaya Aura Communication Manager Local Session Controller.

(6) The UCR 2013, section 3.6.7 includes the On-Site Notification of 911 Call requirements. If the E911 Management System supports notification of a 911 call to a configurable entity within the B/P/C/S or enclave other than a PSAP, such as a front desk or security command center, and the SCs to which the E911 Management System interfaces support notifying the E911 Management System when processing a 911 call, then the E911 Management System shall provide a notification message to a configured non-PSAP entity when a 911 call is made. The SUT met this requirement with testing.

(7) The UCR 2013, section 3.6.8 includes the Internet Protocol version 6 (IPv6) requirements in the subparagraphs below. The SUT met this requirement with testing and the vendor's Letters of Compliance (LoC).

(a) Conformant with Section 5, IPv6, the E911 Management System shall support dual Internet Protocol version 4 (IPv4) and IPv6 stacks (i.e., support both IPv4 and IPv6 in the same IP end point) as described in Request for Comments (RFC) 4213.

(b) The E911 Management System shall meet all of the IPv6 protocol requirements for Network Appliances and Simple Servers (NA/SS) products in Section 5, IPv6, including the requirements in Table 5.2-4, UC Network Appliances and Simple Servers (NA/SS).

(8) The UCR 2013, section 3.6.9 includes the IA requirements. The E911 Management System shall allow an administrator to read, add, delete, and modify the ERL/ELIN entries

maintained in the system. Security testing is accomplished by DISA-led Information Assurance test teams and the results published in a separate report, Reference (d).

(9) The UCR 2013, section 3.6.10 includes the Operation, Administration, Maintenance, and Provisioning (OAM&P) requirements in the subparagraphs below.

(a) The E911 Management System shall allow an administrator to read, add, delete, and modify the ERL/ELIN entries maintained in the system. The SUT met this requirement with testing.

(b) If the E911 Management System interfaces with SCs, then it shall allow an administrator to configure authentication credentials so that the system can authenticate the SCs to which it interfaces, and the SCs can authenticate the E911 Management System. The SUT met this requirement with testing.

(c) If the E911 Management System supports direct, secure electronic transfer of ALI data to a target ALI database, then the E911 Management System shall allow an administrator to configure the address of an ALI database, along with authentication credentials, so that the system can authenticate the ALI database and the ALI database can authenticate the E911 Management System. The SUT met this requirement with testing.

c. Hardware/Software/Firmware Version Identification. Table 3-3 provides the SUT components' hardware, software, and firmware tested. The JITC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

7. TESTING LIMITATIONS. None.

8. CONCLUSION(S). The SUT meets the critical interoperability requirements for an E911 Management System in accordance with the UCR. The SUT was tested with the CS1000M, release Succession Defense Switched Network (DSN) 5.0, and the Avaya Aura Communication Manager (CM), release 6.3.6 with Patch 03.0.124.0-21862 configured with Avaya Enablement (AE) Services, release 6.3.3. The SUT is certified for joint use with any digital switching system or Session Controller that is functionally identical to the CS1000M or Avaya Aura CM configured with Avaya AE Services and is or was on the UC Approved Products List (APL). The SUT meets the interoperability requirements for the interfaces listed in Table 3-1.

DATA TABLES

Table 3-1. SUT Interface Status

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks
Session Controller and Legacy Switch Interfaces			
ISDN T1 PRI NI2 (C)	1 (See note 2.)	Met	The SUT met the critical CRs and FRs for this interface.
Analog (C)	1 (See note 2.)	Met	The SUT met the critical CRs and FRs for this interface, which is used solely for passive call monitoring.
IP (C)	1	Not Tested	The SUT does not support this interface.
SUT Management Interface			
Serial EIA-232 (C)	1	Not Tested	The SUT does not support this interface.
IP (C)	1 (See note 3.)	Met	The SUT met the critical CRs and FRs for this interface.

NOTES:
1. The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3.
2. The SUT is certified for joint use with any digital switching system or Session Controller that is or was previously on the UC APL certified with the ISDN T1 PRI NI2 and analog interfaces.
3. The IP interface was for Operation, Administration, Maintenance, and Provisioning (OAM&P) traffic for SUT management and connectivity to the Avaya Application Enablement (AE) Services, which is connected to the Avaya Aura Communication Manager Session Controller to forward calls to a non-Direct Inward Dial number.

LEGEND:

APL	Approved Products List	ISDN	Integrated Services Digital Network
C	Conditional	NI2	National ISDN Standard 2
CR	Capability Requirements	PRI	Primary Rate Interface
EIA	Electronic Industries Alliance	SUT	System Under Test
FR	Functional Requirements	T1	Digital Transmission Link Level 1
ID	Identification	UC	Unified Capabilities
IP	Internet Protocol	UCR	Unified Capability Requirements

Table 3-2. SUT Capability and Functional Requirements and Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	**E911 Management System Requirements**		
	General E911 Management System (R)	3.6.2	Met
	Automatic Location Identification (ALI) Information (R)	3.6.3	Met
	End Instrument Location at Registration (R)	3.6.4	Met
	Support for ELIN Query at 911 Call (R)	3.6.5	Met
	SC Interfaces with E911 Management Systems (R)	3.6.6	Not Tested (See note 2.)
	On-Site Notification of 911 Call (C)	3.6.7	Met
	IPv6 Support (R)	3.6.8	Met
	Information Assurance (R)	3.6.9	Met (See note 3.)
	Operation, Administration, Maintenance, and Provisioning (OAM&P) (R)	3.6.10	Met

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Table 3-5.
2. This section includes the SC Interfaces with E911 Management Systems requirements. SCs are not required to support interfaces to standalone E911 Management Systems, the burden is on the E911 solution to interface to the SC. However, if an SC does support interfaces to E911 Management Systems, then the requirements in this section apply to the SC. Furthermore, the requirements in this section apply only to SCs that are connected to an active E911 Management System. The requirements in this section do not apply to an E911 Management System. Therefore, the requirements in this section were not tested. However, the SUT met the interface requirements with testing and the vendor's LoC for the ISDN T1 PRI NI2 interface interface while connected to the Avaya CS2100 Multifunction Switch, Avaya CS1000M Small End Office, and Avaya Aura Communication Manager Local Session Controller.
3. Security testing is accomplished by DISA-led Information Assurance test teams and the results published in a separate report, Reference (d).

Table 3-2. SUT Capability and Functional Requirements and Status (continued)

LEGEND:			
C	Conditional	ISDN	Integrated Services Digital Network
CR	Capability Requirement	NI2	National ISDN Standard 2
DISA	Defense Information Systems Agency	PRI	Primary Rate Interface
E911	enhanced emergency service	R	Required
ELIN	Emergency Location Identification Number	SC	Session Controller
FR	Functional Requirement	SUT	System Under Test
ID	Identification	T1	Digital Transmission Link Level 1
IPv6	Internet Protocol version 6	UCR	Unified Capabilities Requirements

Table 3-3. SUT Hardware/Software/Firmware Version Identification

Component	Release	Sub-component	Function
Enterprise Alert Server Dell PE R720	Enterprise Alert 11.11.0.286 EADM Version11.11-Build:25 MS Windows 2012 Server R2 SP2 MS SQL 2012 XnAlert – Version 11.11.0.286 EAFFTmr version 11.11.0.286 Genbridge version 11.0.0.220 genCiscoMon version 11.0.0.10 FW1-Form Version 11.11.0.286 xnGetTMS Version 11.11.0.272 xnupdate Version 11.11.0.272 XnSentry version 11.11.0.286 XnIntradoFTP version 11.0.0.0 WindStreamFtp version 11.0.0.0 FilePurge version 11.11.0.374 Purge911 version 11.11.0.374 Amcom_aes_service version 5.5.0.0 AlwaysUP version 9.0.3.81	AudioCodes (SmartWorks DT6409TE PCIe) digital board and AudioCodes LD809 analog board both with version 5.9.0.3915, firmware 05.03.11 Build 1033	Application/Database Server
Management Server Dell PE R310	11.11-Build:25 Windows 2008 Server R2 SP2 EADM Version 11.11-Build:25	Not Applicable	Management Server
Bypass box	Not Applicable	Not Applicable	Bypass box
Spōk Sentry	MS Windows 7 Professional SP1 XnSentry version 11.11.0.286 XnReport version 11.11.0.272 911play version 11.11.0.374	Not Applicable	Sentry Client Workstation, displays 911 call information

LEGEND:			
APL	Approved Product List	R2	Release 2
E911	enhanced emergency service	SQL	Structured Query Language
EADM	Enterprise Alert Database Management	TDD	Telecommunications Device for the Deaf
MS	Microsoft	UC	Unified Capabilities

Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification

System Name	Software Release	Function
Required Ancillary Equipment (site-provided)		
Active Directory		
Public Key Infrastructure		
Remote Authentication Dial-In User Service (RADIUS)		
Syslogs Server		
Test Network Components (See note.)		
Avaya CS1000M	Succession DSN 5.0	Small End Office
Avaya Aura CM	6.3.6 with Patch 03.0.124.0-21862	Local Session Controller
Avaya Application Enablement (AE) Services	6.3.3	Avaya CM call control adjunct
Avaya CS2100	Succession Enterprise 9.1	Multifunction Switch

NOTE: The SUT was tested with switches listed in this table. JITC analysis determined the SUT is certified with any digital switching system or Session Controller that is or was previously on the UC APL certified with ISDN T1 PRI NI2 and analog interfaces.

LEGEND:

APL	Approved Products List	JITC	Joint Interoperability Test Command
AS	Application Server	NI2	National ISDN Standard 2
CM	Communication Manager	PRI	Primary Rate Interface
DSN	Defense Switched Network	T1	Digital Transmission Link Level 1
ISDN	Integrated Services Digital Network	UC	Unified Capabilities

Table 3-5. E911 Management System Capability/Functional Requirements

ID	Requirement	UCR Ref (See note 1.)	LoC/TP ID (See note 2.)	R/O/C
1	**3.6.2 – General E911 Management System**			
1-1	The E911 Management System shall support signaling interfaces to UC SC products from at least two different vendors, and shall use these interfaces for signaling with those SCs.	3.6.2 AUX-005890	L/T	R
1-2	If the UC SC product supports one or more proprietary signaling interface for E911 Management System interconnection, then the E911 Management System shall support at least one of these interfaces, per the SC vendor's proprietary interface specifications.	3.6.2 AUX-005900	T	C
1-3	If the UC SC product supports one or more standardized signaling interface for E911 Management System interconnection, then the E911 Management System shall support at least one of these interfaces, per standardized interface specifications identified by the SC vendor.	3.6.2 AUX-005910	T	C
2	**3.6.3 – Automatic Location Identification (ALI) Information**			
2-1	The E911 Management System shall maintain, for each SC to which it interfaces, an appropriate set of location data and corresponding ELINs that identify the physical locations of each of the EIs served by the SC.	3.6.3 AUX-005920	T	R
2-2	The E911 Management System shall also maintain any additional data items required by the ALI databases supporting the PSAPs serving the B/P/C/S or enclave. These PSAPs are responsible for handling 911 calls from the EIs served by the SCs to which the E911 Management System interfaces.	3.6.3 AUX-005930	T	R
2-3	The E911 Management System shall be capable of exporting, to a file, ALI data in .csv or National Emergency Number Association (NENA), Version 2.0 or later, formats.	3.6.3 AUX-005940	T	R
2-4	If the B/P/C/S or enclave requires that ALI data be provided in a proprietary format, then the E911 Management System shall be capable of exporting, to a file, the ALI data in the required proprietary format.	3.6.3 AUX-005950	T	C
2-5	If the E911 Management System supports direct, secure electronic transfer of ALI data to a target ALI database (or to an intermediary application or service that in turn updates the ALI database), and the B/P/C/S or enclave supports and allows such a transfer, then a direct electronic export of ALI data shall be allowed in lieu of exporting the data to a file.	3.6.3 AUX-005960	T	C
2-6	The E911 Management System shall be capable of exporting ALI data: a. On a periodic, scheduled basis. b. In response to a configurable event (i.e., the creation of a new ERL and ELIN in the system). c. In response to an administrator's request, on an ad hoc basis.	3.6.3 AUX-005970	T	R
3	**3.6.4 – End Instrument Location at Registration**			
3-1	If the SC provides notification of EI registrations, then the E911 Management System shall do all of the following when notified of an EI registration: a. Determine the physical location of the EI, based on IP address assigned to the EI and any additional information provided by the SC at registration notification. b. Determine the ERL assigned to that location. c. Keep an internal record of the EI registration that includes the ELIN for the ERL assigned to the EI's location. d. Acknowledge receipt of the registration notification to the SC, and include the EI's ELIN in that acknowledgement.	3.6.4 AUX-005980	T	C
3-2	If the EI directly provides notification of registration, then the E911 Management System shall do all of the following when notified of an EI registration: a. Determine the physical location of the EI, based on IP address assigned to the EI and any additional information provided by the EI at registration notification. b. Determine the ERL assigned to that location. c. Keep an internal record of the EI registration that includes the ELIN for the ERL assigned to the EI's location.	3.6.4 AUX-005990	T	C
3-3	When the E911 Management System is unable to determine the location of a registered EI, it shall perform the configured default behavior for this circumstance.	3.6.4 AUX-006000	T	R
4	**3.6.5 – Support for ELIN Query at 911 Call**			
4-1	When queried by an SC processing a 911 call from a registered EI, the E911 Management System shall provide the SC with the ELIN associated with that EI in its internal record.	3.6.5 AUX-006010	T	R

Table 3-5. E911 Management System Capability/Functional Requirements (continued)

ID	Requirement	UCR Ref (See note 1.)	LoC/TP ID (See note 2.)	R/O/C
5	**3.6.6 - SC Interfaces with E911 Management Systems**			
5-1	If the SC proides notification of EI registrations to the E911 Management System, then the SC shall notify the E911 Management System whenever an EI registers with the SC and provide the EI's IP address and a unique identifier for the registration to the E911 Management System with the registration notification.	3.6.6 AUX-006020	T	C
5-2	The SC shall provide additional information, such as the EI's Move, Add, Change (MAC) address, to the E911 Management System with EI registration notification.	3.6.6 AUX-006030	T	O
5-3	If the SC supports receiving and storing, at the EI level, an ELIN provided by an E911 Management System in a response message to a registration notification, then the SC shall do the following: a. Receive the ELIN provided and store it as part of the information maintained for that EI with respect to the registration process. b. Populate the Calling Party Number information element in the ISDN PRI setup message that is sent over the commercial PRI from the SC's MG to the PSTN, with that ELIN, if a 911 call is made from that EI. If the E911 Management system does not respond to an EI's registration notification, or does not provide a valid ELIN in its response, and a 911 call is made from that EI, then the SC shall populate the Calling Party Number information element with the ELIN configured to identify the Default Location for that SC.	3.6.6 AUX-006040	T	C
5-4	If the SC supports querying an E911 Management System during 911 call processing in order to determine the ELIN for the EI from which the 911 call was made, then the SC shall do the following: a. Request the E911 Management System to provide the ELIN for that EI, based on the unique identifier for that EI provided at registration notification. b. The SC shall receive the ELIN provided by the E911 Management System, and populate the Calling Party Number information element in the ISDN PRI setup message, that is sent over the commercial PRI from the SC's MG to the PSTN, with that ELIN. If the E911 Management system does not provide a valid ELIN within a configurable time period, then the SC shall use the ELIN that was configured to identify the Default Location for that SC as the Calling Party Number information element.	3.6.6 AUX-006050	T	C
5-5	If a 911 call is made from an unregistered EI, then the SC shall populate the Calling Party Number information element in the ISDN PRI setup message that is sent over the commercial PRI from the SC's MG to the PSTN, with an ELIN provided by the E911 Management System (either at EI registration or when the 911 call is made) per the default behavior configured in the E911 Management System for this circumstance	3.6.6 AUX-006060	T	R
6	**3.6.7 - On-Site Notification of 911 Call**			
6-1	If the E911 Management System supports notification of a 911 call to a configurable entity within the B/P/C/S or enclave other than a PSAP, such as a front desk or security command center, and the SCs to which the E911 Management System interfaces support notifying the E911 Management System when processing a 911 call, then the E911 Management System shall provide a notification message to a configured non-PSAP entity when a 911 call is made.	3.6.7 AUX-006070	T	C
7	**3.6.8 - IPv6 Support**			
7-1	Conformant with Section 5, IPv6, the E911 Management System shall support dual IPv4 and IPv6 stacks (i.e., support both IPv4 and IPv6 in the same IP end point) as described in RFC 4213.	3.6.8 AUX-006080	L/T	R
7-2	The E911 Management System shall meet all of the IPv6 protocol requirements for Network Appliances and Simple Servers (NA/SS) products in Section 5, IPv6, including the requirements in Table 5.2-4, UC Network Appliances and Simple Servers (NA/SS).	3.6.8 AUX-006090	L/T	R
8	**3.6.9 - Information Assurance**			
8-1	The E911 Management System shall allow an administrator to read, add, delete, and modify the ERL/ELIN entries maintained in the system.	3.6.9 AUX-006100	T	R

Table 3-5. E911 Management System Capability/Functional Requirements (continued)

ID	Requirement	UCR Ref (See note 1.)	LoC/TP ID (See note 2.)	R/O/C
9	**3.6.10 - Operation, Administration, Maintenance, and Provisioning (OAM&P)**			
9-1	The E911 Management System shall allow an administrator to read, add, delete, and modify the ERL/ELIN entries maintained in the system.	3.6.10 AUX-006110	T	R
9-2	If the E911 Management System interfaces with SCs, then it shall allow an administrator to configure authentication credentials so that the system can authenticate the SCs to which it interfaces, and the SCs can authenticate the E911 Management System.	3.6.10 AUX-006120	T	C
9-3	If the E911 Management System supports direct, secure electronic transfer of ALI data to a target ALI database, then the E911 Management System shall allow an administrator to configure the address of an ALI database, along with authentication credentials, so that the system can authenticate the ALI database and the ALI database can authenticate the E911 Management System.	3.6.10 AUX-006130	T	C

NOTES:
1. Refers to the Unified Capabilities Requirements 2013, Errata 1 signed 1 July 2013, Reference (b).
2. Refers to how the requirement is met, either with the vendor's LoC or by testing and cross references the test procedure identification (TP ID) number.

LEGEND:

ALI	Automatic Location Identification	MG	Media Gateway
B/P/C/S	Base/Post/Camp/Station	O	Optional
C	Conditional	PRI	Primary Rate Interface
E911	enhanced emergency service	PSAP	Public Safety Answering Point
EI	End Instrument	PSTN	Public Switched Telephone Network
ELIN	Emergency Location Identification Number	R	Required
ERL	Emergency Response Location	Ref	Reference
IP	Internet Protocol	RFC	Request for Comments
IPv4	Internet Protocol version 4	SC	Session Controller
IPv6	Internet Protocol version 6	T	testable item
ISDN	Integrated Services Digital Network	TP	Test Plan
L	letter item	UC	Unified Capabilities
LoC	Letters of Compliance		

Table 3-6. IPv6 Requirements

ID	Requirement	UCR Ref (See note 1.)	R/C
IP-1	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	5.2.1 IP6-000010	R
IP-2	Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.	5.2.1 IP6-000020	R
IP-3	All nodes and interfaces that are "IPv6-capable" must be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a deliberate transition strategy. This includes the stateless autoconfiguration of link-local addresses. Nodes with multiple network interfaces may need to be separately configured per interface.	5.2.1 IP6-000030	R
IP-4	The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its Approved Products List (APL) category. NOTE: This requirement applies only to products that are required to perform IPv6 functionality.	5.2.1 IP6-000050	R
IP-5	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	5.2.1 IP6-000060	R
IP-6	The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464. NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented.	5.2.1 IP6-000070	R
IP-7	The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095.	5.2.1.1 IP6-000090	R
IP-8	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.	5.2.1.1 IP6-000100	C
IP-9	The product shall not use the Flow Label field as described in RFC 2460.	5.2.1.2 IP6-000110	R

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (See note 1.)	R/C
IP-10	The product shall be capable of setting the Flow Label field to zero when originating a packet.	5.2.1.2 IP6-000120	R
IP-11	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.2.1.2 IP6-000140	R
IP-12	The product shall support the IPv6 Addressing Architecture as described in RFC 4291.	5.2.1.3 IP6-000150	R
IP-13	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.2.1.3 IP6-000160	R
IP-14	If a scoped address (RFC 4007) is used, then the product shall use a scope index value of zero when the default zone is intended.	5.2.1.3 IP6-000170	C
IP-15	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 3315.	5.2.1.4 IP6-000180	C
IP-16	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).	5.2.1.4 IP6-000200	C
IP-17	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.	5.2.1.4 IP6-000220	C
IP-18	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.	5.2.1.4 IP6-000230	C
IP-19	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.	5.2.1.4 IP6-000240	C
IP-20	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.	5.2.1.4 IP6-000250	C
IP-21	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).	5.2.1.4 IP6-000260	C
IP-22	If the product supports DHCPv6 and uses authentication, then it shall discard unauthenticated DHCPv6 messages from UC products and log the event.	5.2.1.4 IP6-000270	C
IP-23	The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.	5.2.1.5 IP6-000280	R
IP-24	The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for any cast addresses or solicited proxy advertisements.	5.2.1.5 IP6-000300	R
IP-25	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.	5.2.1.5 IP6-000310	R
IP-26	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement.	5.2.1.5 IP6-000320	R
IP-27	When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.	5.2.1.5 IP6-000330	R
IP-28	The product shall support the ability to configure the product to ignore Redirect messages.	5.2.1.5.1 IP6-000340	R
IP-29	The product shall only accept Redirect messages from the same router as is currently being used for that destination.	5.2.1.5.1 IP6-000350	R
IP-30	If "Redirect" messages are allowed, then the product shall update its destination cache in accordance with the validated Redirect message.	5.2.1.5.1 IP6-000360	C
IP-31	If the valid "Redirect" message is allowed and no entry exists in the destination cache, then the product shall create an entry.	5.2.1.5.1 IP6-000370	C
IP-32	If redirects are supported, then the device shall support the ability to disable this functionality.	5.2.1.5.1 IP6-000380	C
IP-33	The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.	5.2.1.5.2 IP6-000400	R
IP-34	If the product supports stateless IP address autoconfiguration including those provided for the commercial market, then the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 4862.	5.2.1.6 IP6-000420	C
IP-35	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 autoconfiguration.	5.2.1.6 IP6-000430	C

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (See note 1.)	R/C
IP-36	If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration.	5.2.1.6 IP6-000440	C
IP-37	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. In accordance with RFC 4862, DAD shall be implemented and shall be on by default. Exceptions to the use of DAD are noted in the following text.	5.2.1.6 IP6-000450	R
IP-38	A node MUST allow for autoconfiguration-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.	5.2.1.6 IP6-000460	R
IP-39	The product shall support manual assignment of IPv6 addresses.	5.2.1.6 IP6-000470	R
IP-40	The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.	5.2.1.7 IP6-000520	R
IP-41	The product shall support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.	5.2.1.7 IP6-000540	R
IP-42	The product shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address.	5.2.1.7 IP6-000550	R
IP-43	The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them.	5.2.1.7 IP6-000560	R
IP-44	The product shall support MLD as described in RFC 2710.	5.2.1.8 IP6-000680	R
IP-45	If the product uses IPsec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301.	5.2.1.9 IP6-000690	C
IP-46	If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.	5.2.1.9 IP6-000700	C
IP-47	If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry.	5.2.1.9 IP6-000710	C
IP-48	If RFC 4301 is supported, then the product shall implement IPsec to operate with both integrity and confidentiality.	5.2.1.9 IP6-000720	C
IP-49	If RFC 4301 is supported, then the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.	5.2.1.9 IP6-000730	C
IP-50	If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.	5.2.1.9 IP6-000740	C
IP-51	If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	5.2.1.9 IP6-000750	C
IP-52	If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries, and the product determines it should be discarded, then the product shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPsec protocol if available, source and destination of the packet, and any other selector values of the packet.	5.2.1.9 IP6-000760	C
IP-53	If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS.	5.2.1.9 IP6-000770	C
IP-54	If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.	5.2.1.9 IP6-000780	C
IP-55	If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.	5.2.1.9 IP6-000790	C
IP-56	If RFC 4303 is supported, then the product shall check, as its first check, after a packet has been matched to its SA whether the packet contains a sequence number that does not duplicate the sequence number of any other packet received during the life of the security association.	5.2.1.9 IP6-000800	C
IP-57	If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409.	5.2.1.9 IP6-000810	C
IP-58	To prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.	5.2.1.9 IP6-000820	C
IP-59	If RFC 4301 is supported, then the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.	5.2.1.9 IP6-000830	C
IP-60	If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.	5.2.1.9 IP6-000840	C

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (See note 1.)	R/C
IP-61	If the product supports the IPsec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.	5.2.1.9 IP6-000850	C
IP-62	If RFC 4301 is supported, then the product shall support manual keying of IPsec.	5.2.1.9 IP6-000860	C
IP-63	If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835.	5.2.1.9 IP6-000870	C
IP-64	If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.	5.2.1.9 IP6-000880	C
IP-65	If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.	5.2.1.10 IP6-000990	C
IP-66	If the product uses the Domain Name Service (DNS) resolver for IPv6 based queries, then the product shall conform to RFC 3596 for DNS queries.	5.2.1.10 IP6-001000	C
IP-67	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250-byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the Secure Real-Time Transport Control Protocol (SRTCP) overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	5.2.1.11 IP6-001010	R
IP-68	The product shall forward packets using the same IP version as the version in the received packet.	5.2.1.12 IP6-001040	R
IP-69	When the product is establishing media streams from dual-stacked appliances for AS-SIP signaled sessions, the product shall use the Alternative Network Address Type (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091.	5.2.1.12 IP6-001050	R
IP-70	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a unicast address, then the product shall support generation and processing of unicast IPv6 addresses having the following formats: • x:x:x:x:x:x:x:x (where x is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A. • x:x:x:x:x:x:d.d.d.d (where x is the hexadecimal values of the six high-order 16-bit pieces of the address, and d is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). For example, 1080:0:0:0:8:800:116.23.135.22.	5.2.1.13 IP6-001060	C
IP-71	If the product is using AS-SIP, then the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats: • x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A. • x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22. • compressed zeros: 1080::8:800:200C:417A.	5.2.1.13 IP6-001070	C
IP-72	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), then the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.	5.2.1.13 IP6-001080	C
IP-73	If the product is using AS-SIP, and the <addrtype> is IPv6, then the product shall support the use of RFC 4566 for IPv6 in SDP as described in AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs.	5.2.1.13 IP6-001090	C
IP-74	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is an IPv6 multicast group address, then the multicast connection address shall not have a Time To Live (TTL) value appended to the address as IPv6 multicast does not use TTL scoping.	5.2.1.13 IP6-001100	C
IP-75	If the product is using AS-SIP, then the product shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.	5.2.1.13 IP6-001110	C
IP-76	The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.	5.2.1.14 IP6-001150	R
IP-77	If the product acts as an IPv6 tunnel broker, then the product shall support the function as defined in RFC 3053.	5.2.1.14 IP6-001160	C

Table 3-6. IPv6 Requirements (continued)

ID	Requirement		UCR Ref (See note 1.)	R/C
IP-78	If the system has an IP interface, then the system must be IPv6-capable. Use guidance below from Table 5.2-4 for NA/SS.		Table 5.2-1	R
	RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP	Table 5.2-4	C
	RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	Table 5.2-4	C
	RFC 2409	The Internet Key Exchange (IKE)	Table 5.2-4	C
	RFC 2460	Internet Protocol, Version 6 (IPv6) Specification	Table 5.2-4	R-2
	RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Table 5.2-4	R-3
	RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	Table 5.2-4	R-4
	RFC 2710	Multicast Listener Discovery (MLD) for IPv6	Table 5.2-4	R-8
	RFC 3053	IPv6 Tunnel Broker	Table 5.2-4	C
	RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	Table 5.2-4	C
	RFC 3596	DNS Extensions to Support IPv6	Table 5.2-4	C
	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	Table 5.2-4	C
	RFC 4007	IPv6 Scoped Address Architecture	Table 5.2-4	R
	RFC 4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	Table 5.2-4	R
	RFC 4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	Table 5.2-4	R
	RFC 4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	Table 5.2-4	C
	RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	Table 5.2-4	R-1
	RFC 4291	IP Version 6 Addressing Architecture	Table 5.2-4	R
	RFC 4301	Security Architecture for the Internet Protocol	Table 5.2-4	C
	RFC 4302	IP Authentication Header	Table 5.2-4	C
	RFC 4303	IP Encapsulating Security Payload (ESP)	Table 5.2-4	C
	RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Table 5.2-4	R
	RFC 4566	SDP: Session Description Protocol	Table 5.2-4	C
	RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Table 5.2-4	C
	RFC 4861	Neighbor Discovery for IP Version 6 (IPv6)	Table 5.2-4	R
	RFC 4862	IPv6 Stateless Address Autoconfiguration	Table 5.2-4	C
	RFC 5095	Deprecation of Type 0 Routing Headers in IPv6	Table 5.2-4	R

NOTES:

1. Refers to the Unified Capabilities Requirements 2013, Errata 1 signed 1 July 2013, Reference (b). The individual requirements in this table are not tested. The requirements are met either with the vendor's LoC or by testing over the network configured for IPv4 and then reconfiguring and testing over the network configured for IPv6.

R1. Meets only the dual-stack requirements of this RFC.

R2. Meets only the IPv6 formatting requirements of this RFC.

R3. Meets only the framing format aspects of RFC.

R4. Requirement covered in Section 6, Network Infrastructure End-to-End Performance.

R8. EI (softphones only).

Table 3-6. IPv6 Requirements (continued)

LEGEND:

AH	Authentication Header	kbps	kilobits per second
AS-SIP	Assured Services Session Initiation Protocol	LoC	Letter(s) of Compliance
C	Conditional	MLD	Multicast Listener Discovery
CPE	Customer Premise Equipment	ms	millisecond
DAD	Duplicate Address Detection	MTU	Maximum Transmission Unit
DHCP	Dynamic Host Configuration Protocol	NA/SS	Network Appliance/Simple Server
DHCPv6	Dynamic Host Configuration Protocol for IPv6	R	Required
DNS	Domain Name Service	RFC	Request for Comments
DSCP	Differentiated Services Code Point	SA	Security Architecture
EI	End Instrument	SAD	Security Association Database
ID	Identification	SDP	Session Description Protocol
ICMP	Internet Control Message Protocol	SLAAC	Stateless Address Autoconfiguration
ICMPv6	Internet Control Message Protocol for IPv6	SPD	Security Policy Database
IP	Internet Protocol	TTL	Time To Live
IPSec	Internet Protocol Security	UC	Unified Capabilities
IPv4	Internet Protocol version 4	UCR	Unified Capabilities Requirements
IPv6	Internet Protocol version 6	URI	Uniform Resource Identifiers
ISAKMP	Internet Security Association and Key Management Protocol		