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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) 19 November 2021

MEMORANDUM FOR DISTRIBUTION Revision 1 (See Enclosure 4)

SUBJECT: Joint Interoperability Certification of the Cisco Enterprise Session Controller (ESC) 21 (ESC21) with Software Release 14

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 (UCR 2013) Change 2," September 2017
(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 Department of Defense Information Network (DoDIN) products, Reference (b).

2. **Conditions of Certification.** The Cisco Enterprise Session Controller (ESC) 21 (ESC21) with Software Release 14, hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (b), as an Enterprise Session Controller (ESC) in Type 1, 2, and 3 environments and a Local Session Controller and is certified for joint use with the conditions described in Table 1. This certification expires upon changes that affect interoperability, but no later than the expiration date specified in the DoDIN Approved Products List (APL) memorandum.

Table 1. Conditions

Description		Operational Impact	Remarks
UCR Waivers			
None.			
TDR#	**Conditions of Fielding**		
CIS-0787-005	When an IP EI initiates and establishes a precedence call using a "9P" prefix to an external end instrument on another session controller via an ISDN T1 PRI (ANSI T1.619a), the IP EI is preemptable by callers using the same precedence level or a lesser precedence level. Note, this issue only occurs when the call trunk is over an ISDN T1 PRI and the call is initiated from an IP EI on the SUT.	Minor	CoF: To insure the SUT IP EI is not preemptable by a caller with a lower precedence level, the IP EI must initiate call with the soft-keys on the SUT IP EI in lieu of dialing 9 plus precedence (93, 92, etc.) or configure the IP EI for 2 or more call appearances. Additionally, see note.

(Table continues next page.)

Table 1. Conditions (continued)

Description		Operational Impact	Remarks
TDR#	**Open Test Discrepancies**		
CIS-0787-001	The SUT does not support Preset Conferencing.	Minor	See note.

NOTE(S): DISA accepted the Vendor's POA&M and adjudicated this discrepancy as minor.

LEGEND:

ANSI	American National Standards Institute	POA&M	Plan of Action and Milestones
CIS	Cisco	PRI	Primary Rate Interface
CoF	Condition of Fielding	SS7	Signaling System 7
DISA	Defense Information Systems Agency	SUT	System Under Test
EI	End Instrument	T1	Digital Transmission Link Level 1 (1.544 Mbps)
IP	Internet Protocol	T1.619a	SS7 and ISDN MLPP Signaling Standard for T1
ISDN	Integrated Services Digital Network	TDR	Test Discrepancy Report
Mbps	Megabits per second	UCR	Unified Capabilities Requirements
MLPP	Multi-Level Precedence and Preemption		

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status, Table 3 provides the Capability Requirements and Functional Requirements status, and Table 4 provides the DoDIN APL Product Summary, to include subsequent Desktop Review (DTR) updates.

Table 2. SUT Interface Status

Interface (See note 1.)	Applicability	Status	Remarks
Network Management Interfaces			
10BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3i interface.
100BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3u interface.
1000BaseT	C	Met	The SUT met the critical CRs and FRs for the IEEE 802.3ab interface.
Network Interfaces (Line and Trunk)			
10BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3i interface with the SUT PEIs and softphones.
100BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3u interface with the SUT PEIs and softphones.
1000BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3ab interface with the SUT video PEIs and softphones
2-wire analog	R	Met	The SUT met the critical CRs and FRs for the 2-wire analog interface with the SUT 2-wire secure and non-secure analog instruments.
ISDN BRI	C	Not Tested	The SUT does not support this conditional interface.
Legacy Interfaces (External)			
ISDN T1 PRI (ANSI T1.619a)	R	Partially Met (See note 2.)	The SUT partially met the critical CRs/FRs. This interface provides legacy DSN and TELEPORT connectivity.
ISDN T1 PRI NI-2	R	Met	The SUT met the critical CRs/FRs. This interface provides PSTN connectivity.
T1 CCS7 (ANSI T1.619a)	C	Not Tested	The SUT does not support this conditional interface.
T1 CAS	C	Not Tested	The SUT supports this interface, but it was not tested and not included in this certification.
E1 PRI (ITU-T Q.955.3)	C	Partially Met (See note 2.)	The SUT partially met the critical CRs/FRs. This interface provides OCONUS MLPP connectivity in ETSI-compliant countries.

(Table continues next page.)

Table 2. Interface Status (continued)

Interface (See note 1.)	Applicability	Status	Remarks
Legacy Interfaces (External) (continued)			
E1 PRI (ITU-T Q.931)	C	Met	The SUT met the critical CRs/FRs. This interface provides PSTN connectivity in ETSI-compliant countries.
E1 CAS	C	Not Tested	The SUT supports this interface, but it was not tested and not included in this certification.

NOTE(S):
1. Table 3 depicts the SUT high-level requirements. Refer to Enclosure 3, Table 3-2, for a detailed list of requirements.
2. The SUT met the requirements with the exceptions noted in Table 1. DISA accepted the Vendor's POA&M and adjudicated these exceptions as minor.

LEGEND:

ANSI	American National Standards Institute	Mbps	Megabits per second
BaseT	Megabit Ethernet	MLPP	Multi-Level Precedence and Preemption
BRI	Basic Rate Interface	NI-2	National ISDN Standard 2
C	Conditional	OCONUS	Outside the Continental United States
CAS	Channel Associated Signaling	PEI	Proprietary End Instrument
CCS7	Common Channel Signaling Number 7	POA&M	Plan of Action and Milestones
CR	Capability Requirement	PRI	Primary Rate Interface
DISA	Defense Information Systems Agency	PSTN	Public Switched Telephone Network
DSN	Defense Switched Network	Q.931	Signaling Standard for ISDN
E1	European Basic Multiplex Rate (2.048 Mbps)	Q.955.3	ISDN Signaling Standard for E1 MLPP
ETSI	European Telecommunications Standards Institute	R	Required
FR	Functional Requirement	SS7	Signaling System 7
IEEE	Institute of Electrical and Electronics Engineers	SUT	System Under Test
ISDN	Integrated Services Digital Network	T1	Digital Transmission Link Level 1 (1.544 Mbps)
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	T1.619a	SS7 and ISDN MLPP Signaling Standard for T1

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (See note 1.)	UCR 2013 Reference	Status
1	Voice Features and Capabilities (R)	2.2	Met
2	Assured Services Admission Control (R)	2.3	Met
3	Signaling Protocols (R)	2.4	Met
4	Registration and Authentication (R)	2.5	Met (See note 2.)
5	SC and SS Failover and Recovery (R)	2.6	Met
6	Product Interface (R)	2.7	Met
7	Product Physical, Quality, and Environmental Factors (R)	2.8	Met
8	End Instruments (including tones and announcements) (R)	2.9	Met
9	Session Controller (R)	2.10	Met
10	AS-SIP Gateways (C)	2.11	Not Tested (See note 3.)
11	Enterprise UC Services (R)	2.12	Partially Met (See note 4.)
12	Call Connection Agent (R)	2.14	Met
13	CCA Interaction with Network Appliances and Functions (R)	2.15	Met
14	Media Gateway (R)	2.16	Partially Met (See note 4.)
15	Worldwide Numbering & Dialing Plan (R)	2.18	Met
16	Management of Network Devices (R)	2.19	Met
17	V.150.1 Modem Relay Secure Phone Support (R)	2.20	Met
18	Requirements for Supporting AS-SIP Based Ethernet Devices for Voicemail Systems (C)	2.21	Not Tested (See note 5.)

(Table continues next page.)

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

CR/FR ID	UCR Requirement (See note 1.)	UCR 2013 Reference	Status
19	Local Attendant Console Features (O)	2.22	Not Tested (See note 5.)
20	MSC and SSC (O)	2.23	Not Tested (See note 6.)
21	MSC, SSC, and Dynamic ASAC Requirements in Support of Bandwidth-constrained links (O)	2.24	Not Tested (See note 6.)
22	Other UC Voice (R)	2.25	Partially Met (See note 4.)
23	Cybersecurity Requirements (R)	4	Met (See note 2.)
24	IPv6 Requirements (R)	5	Met
25	Assured Services - Session Initiation Protocol (AS-SIP 2013)	AS-SIP	Met

NOTE(S):
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Reference (c).
2. The JITC-led Cybersecurity test team completed security testing and published the results in a separate report, Reference (d).
3. The SUT was not tested or certified for any of the three optional AS-SIP gateway requirements listed in UCR 2013, Change 2, Section 2.11.
4. The SUT met the requirements with the exceptions noted in Table 1. DISA accepted the Vendor's POA&M and adjudicated these exceptions as minor.
5. The SUT does not support this optional/conditional requirement.
6. This optional requirement applies specifically to a Local Session Controller. The optional requirements for Master Session Controller and Subtended Session Controller were not tested and are not included in this certification.

LEGEND:

ASAC	Assured Services Admission Control	MSC	Master Session Controller
AS-SIP	Assured Services Session Initiation Protocol	O	Optional
C	Conditional	POA&M	Plan of Action and Milestones
CCA	Call Connection Agent	R	Required
CR	Capability Requirement	SC	Session Controller
DISA	Defense Information Systems Agency	SS	Softswitch
FR	Functional Requirement	SSC	Subtended Session Controller
ID	Identification	SUT	System Under Test
IPv6	Internet Protocol version 6	UC	Unified Capabilities
JITC	Joint Interoperability Test Command	UCR	Unified Capabilities Requirements

Table 4. DoDIN APL Product Summary

Product Identification				
Product Name	Cisco ESC 21			
Software Release	14.0.1.11005-1			
UCR Product Type(s)	ESC or LSC			
Product Description	ESC for Type 1, 2, and 3 Environments or as an LSC.			
Product Components	**Component Name** (See notes 1 and 2.)	**Environment**	**Version**	**Remarks**
UCM	**Cisco Unified Communications Manager**	HE, Env 1	14.0.1.11005-1	
Session Management Edition	**Cisco Session Management Edition**	HE	14.0.1.11005-1	
Cisco Unity Connection	**Cisco Unity Connection**	HE, Env 1	14.0.1.10000-19	
Instant Messaging & Presence Server	**Instant Messaging & Presence Server**	HE, Env 1	14.0.1.10000-16	
MCU	**CMS**	HE, Env 1	3.3.0.1	
E911 Management System	**Cisco Emergency Responder**	HE, Env 1	14.0.1.10000-7	
Expressway Control	**Expressway Control Server**	Env 1, 2, 3	x12.6.4	
Expressway Edge	**Expressway Edge Server**	Env 1, 2, 3	x12.6.4	

(Table continues next page.)

Table 4. DoDIN APL Product Summary (continued)

Product Components	Component Name (See notes 1 and 2.)	Environment	Version	Remarks
Customer Premise Equipment	**Cisco UCCX**	HE, Env 1	12.5SU1	
	Cisco Finesse Web Application	Env 1, 2, 3	12.5SU1	
IWG	IWG on 4321 ISR, IWG on the 4461 ISR, IWG on 4331 ISR, IWG on 4351 ISR, IWG on 4431 ISR, **IWG on 4451-X ISR,** IWG on ASR 1001-X, **IWG on ASR 1002-X,** IWG on ASR 1004, IWG on ASR 1006, IWG on ASR 1006-X	HE, Env 1, 2	IOS XE 17.03.03	
IWG	**IWG on CSR-1000v**	HE, Env 1, 2	IOS XE 17.03.03	
SBC	SBC on 4321 ISR, SBC on the 4461 ISR, SBC on 4331 ISR, SBC on 4351 ISR, SBC on 4431 ISR, **SBC on 4451-X ISR,** SBC on ASR 1001-X, **SBC on ASR 1002-X,** SBC on ASR 1004, SBC on ASR 1006, SBC on ASR 1006-X	HE, Env 1, 2	IOS XE 17.03.03	
SBC	**SBC on CSR-1000v**	HE, Env 1, 2	IOS XE 17.03.03	
IWG/SBC	IWG/SBC on 4321 ISR, IWG/SBC on the 4461 ISR, IWG/SBC on 4331 ISR, IWG/SBC on 4351 ISR, IWG/SBC on 4431 ISR, **IWG/SBC on 4451-X ISR,** IWG/SBC on ASR 1001-X, **IWG/SBC on ASR 1002-X,** IWG/SBC on ASR 1004, IWG/SBC on ASR 1006, IWG/SBC on ASR 1006-X	HE, Env 1, 2	IOS XE 17.03.03	
IWG/SBC	**IWG/SBC on CSR-1000v**	HE, Env 1, 2	IOS XE 17.03.03	
Media Gateway	4321 ISR, 4331 ISR, 4351 ISR, 4431 ISR, **4451-X ISR,** 4461 ISR with the following T1/E1 cards: **NIM-2MFT T1/E1**, NIM-1MFT-T1/E1, NIM-4MFT-T1/E1, NIM-8MFT-T1/E1	HE, Env 1, 2	IOS XE 17.03.03	
Analog Voice Gateway	**VG450** with the following service and network interface modules**: SM-X-72FXS,** SM-X-8FXS/12FXO, SM-X-16FXS/2FXO, SM-X-24FXS/4FXO, **NIM-4FXSP,** NIM-2FXSP	Env 1, 2	IOS XE 17.03.03	
Media Termination Point (MTP)	Media Termination Point on 4321 ISR Media Termination Point on 4331 ISR Media Termination Point on 4351 ISR Media Termination Point on 4431 ISR **Media Termination Point on 4451-X ISR** Media Termination Point on 4461 ISR	HE, Env 1, 2	IOS XE 17.03.03	
Jabber (Voice and Video Soft Client)	**Cisco Jabber for Windows**	Env 1, 2, 3	14.0.1.55914 (Build 305914) (Windows 10)	
IP Phone (Voice)	**IP Phone 7811**	Env 1, 2, 3	sip78xx.14-0-1-0001-135	
IP Phone (Voice)	IP Phone 7821	Env 1, 2, 3	sip78xx.14-0-1-0001-135	
IP Phone (Voice)	**IP Phone 7841**	Env 1, 2, 3	sip78xx.14-0-1-0001-135	
IP Phone (Voice)	IP Phone 7861	Env 1, 2, 3	sip78xx.14-0-1-0001-135	
IP Phone Tempest	IP Phone 88XX	Env 1, 2, 3	sip78xx.14-0-1-0001-135	
IP Phone (Voice and Video)	Unified IP Phone 8811	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	Unified IP Phone 8831 Conference Phone	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	API EM-8831-xx	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	Unified IP Phone 8851 and 8851NR	Env 1, 2, 3	sip88xx.12-7-1-0001-393	
IP Phone (Voice and Video)	API EM-8851–xx	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	CIS DTD-8851-01	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	**Unified IP Phone 8841**	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	API EM-8841–xx	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	API EL1-8841–xx	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	CIS DTD-8841-01	Env 1, 2, 3	sip88xx.14-0-1-0001-135	

(Table continues next page.)

Table 4. DoDIN APL Product Summary (continued)

Product Components	**Component Name** (See notes 1 and 2.)	**Environment**	**Version**	**Remarks**
IP Phone (Voice and Video)	CIS DTD-8841T-01-L1	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	CIS DTD-8841-02	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
Conference Phone	Cisco IP Conference Phone 8832	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	**Unified IP Phone 8845**	Env 1, 2, 3	sip8845_65.14-0-1-0001-135	
IP Phone (Voice and Video)	Unified IP Phone 8861	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
IP Phone (Voice and Video)	**Unified IP Phone 8865,** 8865NR	Env 1, 2, 3	sip8845_65.14-0-1-0001-135	
Expansion Module	Unified IP Phone KEM Expansion module for 8800 series IP Phones	Env 1, 2, 3	Not Applicable	
Conference Phone	Cisco IP Conference Phone 8832	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
Conference Phone	Cisco IP Conference Phone 8832 NR	Env 1, 2, 3	sip88xx.14-0-1-0001-135	
Conference Phone	Cisco IP Conference Phone 7832	Env 1, 2, 3	sip78xx.14-0-1-0001-135	
Video Teleconference	Cisco Webex Room 55, Cisco Webex Room 55 Single NR, Cisco Webex Room 55 Dual, Cisco Webex Room 55 Dual NR, Cisco Webex Room 70G2 Single, Cisco Webex Room 70 G2 Single NR, Cisco Webex Room 70 G2 Dual NR, Cisco Webex Room 70d, Cisco Webex Room 70s Endpoints	Env 1, 2, 3	CE 9.14.6-cf0c4696851-2021-03-26	
Video Teleconference	Cisco Webex Room Kit, Cisco Webex Room Kit NR**, Cisco Webex Room Kit Mini**, Cisco Webex Room Kit Mini NR, Cisco Webex Room Kit Plus, Cisco Webex Room Kit Plus NR, Cisco Webex Room Kit Pro, Cisco Webex Room Kit Pro NR Endpoints	Env 1, 2, 3	CE 9.14.6-cf0c4696851-2021-03-26	
Video Teleconference	Cisco Webex Board 55, Cisco Webex Board 55S, Cisco Webex Board 70, Cisco Webex Board 70S, and Cisco Webex Board 85S Endpoints	Env 1, 2, 3	CE 9.14.6-cf0c4696851-2021-03-26	
Video Teleconference	**Cisco Webex Desk Pro**, Cisco Webex Desk Pro NR Endpoints	Env 1, 2, 3	CE 9.14.6-cf0c4696851-2021-03-26	
Video Teleconference	Cisco Webex Room Panorama, Cisco Webex Room Panorama NR, Cisco Webex Room 70 Panorama, and Cisco Webex Room 70 Panorama NR endpoints	Env 1, 2, 3	CE 9.14.6-cf0c4696851-2021-03-26	
Video Teleconference	Cisco Webex Room 70S NR and Cisco Webex Room 70D NR Endpoints	Env 1, 2, 3	CE 9.14.6-cf0c4696851-2021-03-26	
Analog PSTN mode DSCD	**GD vIPer**	Env 1, 2, 3	6.1.2.1 (See note 3.)	Site-Provided
SCCP and SIP modes DSCD	**GD IP vIPer**	Env 1, 2, 3	6.1.2.1 (See note 3.)	Site-Provided

NOTE(S):
1. Components bolded and underlined were tested by JITC. The other components in the family series were not tested but are also certified for joint use. JITC certifies those additional components because they utilize the same software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.
2. A comprehensive list of supported hardware configurations can be found by selecting the "Cisco Unified Communications on the Cisco Unified Computing System" link at the following URL: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html.
3. Although the SUT was tested and is certified with this GD vIPer DSCD version, based on JITC analysis the SUT is also certified with other versions previously and currently listed on the DoDIN APL as denoted under a separate Tracking Number for the GD vIPer DSCD.

(Table continues next page.)

Table 4. DoDIN APL Product Summary (continued)

LEGEND:

API	Application Programming Interface	ISR	Integrated Services Router
APL	Approved Products List	IWG	Interworking Gateway
ASR	Aggregated Services Router	JITC	Joint Interoperability Test Command
CE	Collaboration Endpoint	KEM	Key Expansion Module
CIS	Cisco	LSC	Local Session Controller
CMS	Cisco Meeting Server	MCU	Multipoint Conference Unit
CSR	Cisco Cloud Services Router	MTP	Media Termination Point
DoDIN	Department of Defense Information Network	NR	No Radio
DSCD	DoD Secure Communications Device	PSTN	Public Switched Telephone Network
E911	Enhanced 911	SBC	Session Border Controller
Env	Environment (Type 1, 2, 3)	SCCP	Skinny Call Control Protocol
ESC	Enterprise Session Controller	SIP/sip	Session Initiation Protocol
GD	General Dynamics	UCCX	Unified Contact Center Express
HE	Head End	UMC	Unified Communications Manager
IOS	Internetwork Operating System	URL	Uniform Resource Locator
IP	Internet Protocol	vIPer	Voice over IP Encryptor

4. Test Details. This certification is based on interoperability testing, review of the Vendor's Letters of Compliance (LoC), Defense Information Systems Agency (DISA) adjudication of open test discrepancy reports (TDRs), and the DISA Certifying Authority Recommendation for inclusion on the DoDIN APL. Conducted testing at JITC's Global Network Test Facility at Fort Huachuca, Arizona, from 7 June through 24 June 2021, using test procedures derived from Reference (c). Additionally, verification and validation testing was conducted from 23 through 27 August to resolve and close several interoperability issues. The review of the Vendor's LoC was completed on 5 May 2021. DISA adjudicated outstanding TDRs on 14 September 2021. The JITC-led Cybersecurity test team completed security testing and published the results 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. Enclosure 4 provides a list of errata changes to this extension since the original signature date.

5. Additional Information. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (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 Industry Toolkit (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the CS Assessment Package that contains the approved configuration and deployment guide must be requested directly from the Approved Products Certification Office (APCO) via e-mail: disa.meade.ie.list.approved-products-certification-office@mail.mil. All associated information is available on the DISA APCO website located at https://aplits.disa.mil/.

6. Point of Contact (POC). JITC POC: Ms. Elaine Macari, commercial telephone (520) 538-5483, DSN telephone 879-5483, FAX DSN 879-4347; e-mail address: elaine.s.macari.civ@mail.mil; mailing address: Joint Interoperability Test Command, ATTN: JTE2 (Ms. Elaine Macari), P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The APCO tracking number for the SUT is 2104001.

FOR THE COMMANDER:

CLARK.BRADLEY.ALAN.1231466564 Digitally signed by CLARK.BRADLEY.ALAN.1231466564 Date: 2021.11.19 08:47:20 -07'00'

4 Enclosures a/s

for LAWRENCE T. DORN
Chief
Networks/Communications &
DoDIN Capabilities Division

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
ISG Secretariat, DISA, JT
U.S. Strategic Command, J66
USSOCOM J65
USTRANSCOM J6
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6, SAIS-CBC
US Air Force, SAF/A6SA
US Marine Corps, MARCORSYSCOM, SEAL, CERT Division
US Coast Guard, CG-64
DISA/ISG REP
OUSD Intel, IS&A/Enterprise Programs of Record
DLA, Test Directorate, J621C
NSA/DT
NGA, Compliance and Assessment Team
DOT&E
Medical Health Systems, JMIS PEO T&IVV
HQUSAISEC, AMSEL-IE-IS
APCO

ADDITIONAL REFERENCES

(c) Joint Interoperability Test Command (JITC), “Enterprise Session Controller (SC) Test Procedures Version 1.0 for Unified Capabilities Requirements (UCR) 2013 Change 2,” August 2019
(d) JITC, “Cybersecurity Assessment Report For Cisco Enterprise Session Controller (ESC) 21, Software Release 14, Tracking Number (TN) 2104001,” May 2021

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Cisco Enterprise Session Controller (ESC) 21 (ESC21) with Software Release 14 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	Defense Information Systems Agency (DISA)
Sponsor Point of Contact	James Marshall, email: james.e.marshall.civ@mail.mil, Phone: 301-225-3506
Vendor Point of Contact	Ryan Nottingham, e-mail: rnotting@cisco.com, Phone: 520-452-4389
System Name	Cisco Enterprise Session Controller (ESC) 21 (ESC21)
Increment and/or Version	Software Release 14
Product Category	ESC and Local Session Controller
System Background	
Previous certifications	TN1525401, TN1331201
Tracking	
APCO ID	2104001
System Tracking Program ID	10594
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Change 2, Sections 2, 4, and 5
Remarks	None
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona

LEGEND:
APCO Approved Products Certification Office
DISA Defense Information Systems Agency
ESC Enterprise Session Controller
ID Identification
TN Tracking Number

2. SYSTEM DESCRIPTION. The Enterprise Unified Capabilities (UC) Services Architecture consists of ESC Core Infrastructure products at a centralized "Master Site" location and Edge Infrastructure products at Department of Defense (DoD) Components' Base/Post/Camp/Station (B/P/C/S) locations. The ESC Core Infrastructure is composed of centralized ESC components, an ESC-fronting Session Border Controller (SBC), Enterprise Hosted UC Services, and Enterprise Required Ancillary Equipment (RAE). The Edge Infrastructure consists of End Instruments (EIs), Media Gateways (MGs), Enclave-fronting SBCs, local survivable call processing appliances (for Types 1 and 2), and local RAE. The geographic region that encompasses the centralized ESC location together with all of the served DoD Components B/P/C/S locations is referred to as the Enterprise Services Area (ESA). The ESC provides an integrated management framework that enables the centralized configuration, provisioning, administration, management, and monitoring of all Centralized Enterprise Services Infrastructure components and all Edge Infrastructure components within the ESA. Reliable and redundant systems at all levels of the Enterprise UC Services architecture ensure the high availability needed to meet the requirements of the warfighter and operational user. The ESC provides centralized, integrated voice, video, and data session management on behalf of served Internet

Protocol (IP) EIs located at different enclaves (i.e., B/P/C/S locations) within the served geographic region. A full suite of Enterprise Hosted UC Services is collocated with the ESC.

The Hosted UC Services include the following:

- Voice and video session management.
- Voice and video conferencing.
- Unified messaging.
- E911 Call Management.
- Extensible Messaging and Presence Protocol (XMPP) Instant Messaging (IM)/Chat/Presence federation.
- Enterprise Directory Services.

The ESC21 Unified Communications solution will be installed on the Cisco Hyperflex Server platforms or equivalent hardware. A comprehensive list of supported hardware configurations can be found by selecting the "Cisco Unified Communications on the Cisco Unified Computing System" link at the following Uniform Resource Locator (URL): https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html. The Cisco Unified Communications Manager (UCM) supports multiple types of user EI connections types. These include Internet Protocol (IP) phones (both hardware and software based), Cisco Jabber clients, analog devices connected to an Integrated Services Router or to a Voice Gateway (VG), and non-assured H.323 devices. Optional H.323 capabilities are provided through the use of the Cisco Expressway Server; however, H.323 was not tested and is not included in this certification. The Cisco 4000 series Integrated Routers are used as Voice over IP (VoIP) gateways with traditional Time Division Multiplexing (TDM) circuits such as T1 (Digital Transmission Link Level 1 (1.544 Megabits per second (Mbps))/E1 (European Basic Multiplex Rate (2.048 Mbps)) trunks.

The management interface for the Session Management Edition (SME) is a web-based administrative console. To access it, a management user will connect to the device using Public Key Infrastructure (PKI) for authentication from a Security Technical Implementation Guideline (STIG) compliant management workstation.

The SUT is certified for joint use as an ESC in Type 1, 2, and 3 environments and as a Local Session Controller (LSC).

Head End Components:

Cisco Unity Connection (CUC) – The CUC provides voicemail and Unified Messaging. Users can access Cisco CUC with multiple methods, including a phone interface, Web Interface, and visual voicemail (Jabber Applications). The CUC supports full Unified Messaging for voicemail to email delivery by integrating with Microsoft Exchange through Exchange Web Services.

Cisco Meeting Server – The Cisco Meeting Server is software that can be run on its own optimized platform, or on Cisco Unified Computing System (UCS) hardware, and other supported third-party servers as a virtual machine. As a virtual machine it is supported on multiple versions of Elastic Sky X infrastructure (ESXi). The Cisco Meeting Server 3.3 software provides audio and video conferencing services within the ESC head-end architecture for this solution. A comprehensive list of supported ESXi and hardware configurations can be found by selecting the "Cisco Unified Communications on the Cisco Unified Computing System" link at the following URL: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html.

Cisco Emergency Responder (CER) 911 – The CER 911 provides reliable user location information to the Public Safety Access Point (PSAP) when a subscriber calls 911 from the Cisco ESC. The Cisco CER 911 allows administrators to define Emergency Response Locations (ERLs) based on either location or IP addressing, and corresponding physical location (Automatic Location Identification (ALI)), to alert local and PSAP teams of an emergency call. The CER 911 also allows for routing any PSAP call back to the IP phone, which dialed 911.

Cisco UCM SME Cluster (Pub and Sub) – The UCM provides VoIP call processing, call admission control, messaging, identification, authentication, and security services to users. The Pub and Subs are installed as VMs within the SUT. The SME provides for a simplified Enterprise Management approach for deploying multiple clusters in the ESC and interconnecting them back into a centralized call routing/call control solution.

Interworking Gateway (IWG)/SBC – The IWG deployment as part of the ESC provides critical Session Initiation Protocol (SIP) message normalization functionality that allows interoperability between components within the UC architecture. The Cisco IWG is an integrated Cisco Internetwork Operating System (IOS) software application that runs on the 4000 ISR series, Aggregation Services Router (ASR) 1000 series, and Cloud Services Router (CSR) 1000v routers. The Cisco CSR 1000v is a software router that is deployed on a VM instance x86 server hardware. It can run on the Cisco UCS server, as well as servers from other vendors. The CSR 1000v was tested on a ESXi 6.5 VM server host. The IWG can be deployed in pairs to provide high availability. This is accomplished by using Hot Standby Routing Protocol (HSRP). The SBC deployment as part of the ESC provides critical SIP message normalization functionality that allows interoperability between components with the UC architecture. The Cisco SBC is an integrated IOS software application that runs on the Cisco 4000 ISR series, ASR 1000 series, and CSR-1000v routers. The SBC can be deployed in pairs to provide high availability. This is accomplished by using HSRP.

Type 1 Sites UCM (Pub) – The UCM provides VoIP call processing, call admission control, messaging, identification, authentication, and security services to users. The Pub and Subs are installed on VMs within the SUT.

Type 2 Managed Services Cisco Instant Messaging and Presence (IM&P) – The Cisco IM&P provides IM&P using native XMPP clients, capable of integrating with a SIP simple

Type. The IM&P supports a distributed cluster model. Multiple nodes of IM&P provide inter-domain federation and scale seamlessly through full XMPP inter-domain federation.

Type 2 Managed Services Cisco Unified Contact Center Express (UCCX) – The Cisco UCCX provides a multimedia IP-enabled customer-care application Type that enhances the efficiency of contact centers by simplifying business integration, easing agent administration, increasing agent flexibility, and enhancing network hosting. The Cisco UCCX is a proprietary contact center solution that is subtended to a Cisco Session Controller. The Cisco UCCX is the application host server for the Cisco Finesse contact center application. The Cisco UCCX is installed as a VM within the SUT.

Type 2 Managed Services UCM Cluster (Pub and Sub) – The UCM provides VoIP call processing, call admission control, messaging, identification, authentication, and security services to users. The Pub and Subs are installed as VMs within the SUT.

Type 3 Managed Services IWG/SBC – The IWG deployment as part of the ESC provides critical SIP message normalization functionality that allows interoperability between components within the UC architecture. The Cisco IWG is an integrated Cisco IOS software application that runs on the Cisco 4000 ISR series, ASR 1000 series, and CSR 1000v routers. The Cisco CSR 1000v is a software router that is deployed on a VM instance x86 server hardware. It can run on Cisco UCS server, as well as servers from other vendors. The CSR 1000v was tested on a ESXi 6.5 VM server host. The IWG can be deployed in pairs to provide high availability. This is accomplished by using HSRP. The SBC deployment as part of the ESC provides critical SIP message normalization functionality that allows interoperability between components with the UC architecture. The Cisco SBC is an integrated IOS software application that runs on the Cisco 4000 ISR series, ASR 1000 series, and CSR-1000v routers. The SBC can be deployed in pairs to provide high availability. This is accomplished by using HSRP.

Type 3 Managed Services Cisco IM&P – The Cisco IM&P provides IM&P using native XMPP clients, capable of integrating with a SIP Simple environment for interoperability. The IM&P supports a distributed cluster model. Multiple nodes of IM&P provide intra-domain federation and scale seamlessly through full XMPP inter-domain federation.

Type 3 Managed Services UCCX – The Cisco UCCX provides a multimedia IP-enabled customer-care application environment that enhances the efficiency of contact centers by simplifying business integration, easing agent administration, increasing agent flexibility, and enhancing network hosting. The Cisco UCCX is a proprietary contact center solution that is subtended to a Cisco Session Controller. The Cisco UCCX is the application host server for the Cisco Finesse contact center application. The Cisco UCCX is installed as a VM within the SUT.

Type 3 Managed Services Media Termination Point (MTP) – The MTP is an IOS XE based gateway that converts IP version 6 (IPv6) to IP version 4 (IPv4) and vice versa.

Type 3 Managed Services MG – The MG is an ISR 4451. The Cisco ISR 4000 Series voice gateway (GW) provides connectivity to traditional TDM components to the VoIP network. These MGs host both analog interfaces and T1/E1 trunk circuits**.**

Type 3 Managed Services UCM Cluster (Pub and Sub) – The UCM provides VoIP call processing, call admission control, messaging, identification, authentication, and security services to users. The Pub and Subs are installed as VMs within the SUT.

Management Workstation (Site-Provided) – Windows 10 workstation.

ESC Type 1 Environment Components:

IP Phones 88XX Series/88xx Series Tempest Devices – The 88xx series IP phones are programmed from the UCM Cluster as Proprietary End Instrument (PEI) devices. Configuration and individual user features are selected from the UCM application. Models included in this series are the 8811, 8831, 8841, 8845, 8851, 8851 No Radio (NR), 8861, 8865. There are 88XX Series Tempest hardened versions of these phones certified by similarity. These provide security protections compliant with Committee on National Security Systems Instruction (CNSSI) 5001 for use Sensitive Compartmented Information Facility (SCIF), and Special Access Program Facility (SAPF) environments.

Cisco Webex Devices – The Webex endpoints are video enabled IP phones and are programmed from the UCM Cluster PEI devices, and the features are selected for the individual user from the UCM application.

Unified IP Color Key Expansion Module (KEM) 8800 Series – The 8800 series KEM is for the Unified IP phone 88xx series (with a maximum of two per phone).

IP Phones 78XX Series – The 7811, 7821, 7841, and 7861 IP phones are programmed from the UCM Cluster as PEIs, and the features are selected for the individual user from the UCM application.

Type 1 UCM Cluster (Sub) – The UCM provides VoIP call processing, call admission control, messaging, identification, authentication, and security services to users. The Pub and Subs are installed as VMs within the SUT.

IWG/SBC – The IWG deployment as part of the ESC provides critical SIP message normalization functionality that allows interoperability between components within the UC architecture. The Cisco IWG is an integrated Cisco IOS software application that runs on the 4000 ISR series, ASR 1000 series, and CSR 1000v routers. The Cisco CSR 1000v is a software router that is deployed on a VM instance x86 server hardware. It can run on Cisco UCS server, as well as servers from other vendors. The CSR 1000v was tested on a ESXi 6.5 VM server host. The IWG can be deployed in pairs to provide high availability. This is accomplished by using HSRP. The SBC deployment as part of the ESC provides critical SIP message normalization functionality that allows interoperability between components with the UC architecture. The Cisco SBC is an integrated IOS Software application that runs on the Cisco 4000 ISR series, ASR 1000 series, and CSR-1000v routers. The SBC can be deployed in pairs to provide high availability. This is accomplished by using HSRP.

CER 911 – The CER 911 provides reliable user location information to the Public Safety Access Point (PSAP) when a subscriber calls 911 from the Cisco ESC. The Cisco CER 911 allows administrators to define ERLs based on either location or IP addressing, and corresponding physical location (ALI), to alert local and PSAP teams of an emergency call. CER 911 also allows for routing any PSAP call back to the IP phone, which dialed 911.

Cisco IM&P – The Cisco IM&P provides IM&P using native XMPP clients, capable of integrating with a SIP Simple environment for interoperability. The IM&P supports a distributed cluster model. Multiple nodes of IM&P provide intra-domain federation and scale seamlessly through full XMPP inter-domain federation.

Unified Contact Center Express – The Cisco UCCX provides a multimedia IP-enabled customer-care application environment that enhances the efficiency of contact centers by simplifying business integration, easing agent administration, increasing agent flexibility, and enhancing network hosting. The Cisco UCCX is a proprietary contact center solution that is subtended to a Cisco Session Controller. The UCCX is the application host server for the Cisco Finesse contact center application. The UCCX is installed as a VM within the SUT.

MTP – The MTP is an IOS XE based gateway that converts IPv6 to IPv4 and vice versa.

Cisco Jabber for Windows – Provides the main workspace application for the ESC. It enhances productivity by unifying presence, IM, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one client on a user's desktop. The Cisco Jabber for Windows delivers highly secure, clear, and reliable communications. It offers flexible deployment models, is built on open standards, and integrates with commonly used desktop applications. The Cisco Jabber client can also connect remotely to the ESC 21 through the Cisco Expressway Advanced Collaboration GW.

VG – The Voice Gateway is a VG450. The Cisco VG450 High Density Analog Gateway is a Cisco IOS XE Software based analog phone gateway. It connects analog phones to an enterprise voice system based on Cisco UCM. The VG450 is operating as a high-density analog voice EI GW only with no support for fax or V.150.

MG – The MG is a ISR 4451. The Cisco ISR 4000 Series voice GW provides connectivity to traditional TDM components to the VoIP network. These MGs host both analog interfaces and T1/E1 trunk circuits.

Cisco Finesse – The Cisco Finesse integrates traditional contact center functions into a thin-client desktop. It implements a browser-based desktop through a web interface, no client-side installations required. The Cisco Finesse application is hosed on the UCCX and accessed using site provided, STIG compliant, Common Access Card (CAC)-enabled Windows workstation to browse to the UCCX and run the Finesse web application.

Expressway – Expressway provides the ability for Cisco EIs and clients outside the firewall, to access highly secure collaboration workloads, including XMPP, voice and video within ESC21 without the need of a Virtual Private Network (VPN). The Expressway feature is broken up over two servers.

- **The Expressway Edge Server** – The Expressway Edge sits in the Demilitarized zone (DMZ) and proxies all of the traffic from outside the firewall into the internal network.
- **The Expressway Control Server** – The Expressway Control server sits inside the network and connects to the Expressway Edge.

Cisco Webex Devices – The Webex endpoints are video enabled IP phones and are programmed from the UCM Cluster PEI devices, and the features are selected for the individual user from the UCM application.

ESC Type 2 Environment Components:

IP Phones 88XX Series/88xx Series Tempest Devices – The 88xx series IP phones are programmed from the UCM Cluster as PEI devices. Configuration and individual user features are selected from the UCM application. Models included in this series are the 8811, 8831, 8841, 8845, 8851, 8851 NR, 8861, 8865. There are 88XX Series Tempest hardened versions of these phones certified by similarity. These provide security protections compliant with CNSSI 5001 for use in SCIF, and SAPF environments.

Cisco Webex Devices – The Webex endpoints are video enabled IP phones and are programmed from the UCM Cluster PEI devices, and the features are selected for the individual user from the UCM application.

Unified IP Color KEM 8800 Series – The 8800 series KEM is for the Unified IP Phone 88xx series (with a maximum of two per phone).

IP Phones 78XX Series – The 7811, 7821, 7841, and 7861 IP phones are programmed from the UCM Cluster as PEIs, and the features are selected for the individual user from the UCM application.

IWG/SBC – The IWG deployment as part of the ESC provides critical SIP message normalization functionality that allows interoperability between components within the UC architecture. The Cisco IWG is an integrated Cisco IOS software application that runs on the 4000 ISR series, ASR 1000 series, and CSR 1000v routers. The Cisco CSR 1000v is a software router that is deployed on a virtual machine (VM) instance x86 server hardware. It can run on Cisco UCS server, as well as servers from other vendors. The CSR 1000v was tested on a ESXi 6.5 VM server host. The IWG can be deployed in pairs to provide high availability. This is accomplished by using HSRP. The SBC deployment as part of the ESC provides critical SIP message normalization functionality that allows interoperability between components with the UC architecture. The Cisco SBC is an integrated IOS Software application that runs on the 4000 ISR series, ASR 1000 series, and CSR-1000v routers. The SBC can be deployed in pairs to provide high availability. This is accomplished by using HSRP.
MTP – The MTP is an IOS XE based gateway that converts IPv6 to IPv4 and vice versa.

Cisco Jabber for Windows – Provides the main workspace application for the ESC. It enhances productivity by unifying presence, IM, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one client on a user's desktop. CISCO Jabber for Windows delivers highly secure, clear, and reliable communications. It offers flexible deployment models, is built on open standards, and integrates with commonly used desktop applications. The CISCO Jabber client can also connect remotely to the ESC 21 through the CISCO Expressway Advanced Collaboration GW.

MG – The MG is an ISR 4451. The Cisco ISR 4000 Series voice GW provides connectivity to traditional TDM components to the VoIP network. These MGs host both analog interfaces and T1/E1 trunk circuits.

Cisco Finesse – The Cisco Finesse integrates traditional contact center functions into a thin-client desktop. It implements a browser-based desktop through a web interface, no client-side installations required. The Cisco Finesse application is hosed on the UCCX and accessed using site provided, STIG compliant, CAC-enabled Windows workstation to browse to the UCCX, and run the Finesse web application.

Cisco Webex Devices – The Webex endpoints are video enabled IP phones and are programmed from the UCM Cluster PEI devices, and the features are selected for the individual user from the UCM application.

Expressway – Expressway provides the ability for Cisco end instruments and clients outside the firewall, to access highly secure collaboration workloads, including XMPP, voice and video within ESC21 without the need of a VPN. The Expressway feature is broken up over two servers.

- **The Expressway Edge Server** – The Expressway Edge sits in the DMZ and proxies all of the traffic from outside the firewall into the internal network.
- **The Expressway Control Server –** The Expressway Control server sits inside the network and connects to the Expressway Edge.

ESC Type 3 Environment Components:

IP Phones 88XX Series/88xx Series Tempest Devices – The 88xx series IP phones are programmed from the UCM Cluster as PEI devices. Configuration and individual user features are selected from the UCM application. Models included in this series are the 8811, 8831, 8841, 8845, 8851, 8851 NR, 8861, 8865. There are 88XX Series Tempest hardened versions of these phones certified by similarity. These provide security protections compliant with CNSSI 5001 for use in SCIF, and SAPF environments.

Cisco Webex Devices – The Webex endpoints are video enabled IP phones and are programmed from the UCM Cluster PEI devices, and the features are selected for the individual user from the UCM application.
Unified IP Color KEM 8800 Series – The 8800 series KEM is for the Unified IP Phone 88xx series (with a maximum of two per phone).

IP Phones 78XX Series – The 7811, 7821, 7841, and 7861 IP phones are programmed from the UCM Cluster as PEIs, and the features are selected for the individual user from the UCM application.

Cisco Jabber for Windows – Provides the main workspace application for the ESC. It enhances productivity by unifying presence, IM, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one client on a user's desktop. The Cisco Jabber for Windows delivers highly secure, clear, and reliable communications. It offers flexible deployment models, is built on open standards, and integrates with commonly used desktop applications. The Cisco Jabber client can also connect remotely to the ESC 21 through the Cisco Expressway Advanced Collaboration GW.

Cisco Finesse – The Cisco Finesse integrates traditional contact center functions into a thin-client desktop. It implements a browser-based desktop through a web interface, no client-side installations required. The Cisco Finesse application is hosed on the UCCX and accessed using site provided, STIG compliant, CAC-enabled Windows workstation to browse to the UCCX, and run the Finesse web application.

Cisco Webex Devices – The Webex endpoints are video enabled IP phones and are programmed from the UCM Cluster PEI devices, and the features are selected for the individual user from the UCM application.

Expressway – Expressway provides the ability for Cisco end instruments and clients outside the firewall, to access highly secure collaboration workloads, including XMPP, voice and video within ESC21 without the need of a VPN. The Expressway feature is broken up over two servers.

- **The Expressway Edge Server** – The Expressway Edge sits in the DMZ and proxies all of the traffic from outside the firewall into the internal network.
- **The Expressway Control Server** – The Expressway Control server sits inside the network and connects to the Expressway Edge.

Endpoints Certified with Expressway:

IP Phones 88XX Series/88xx Series Tempest Devices – The 88xx series IP phones are programmed from the UCM Cluster as PEI devices. Configuration and individual user features are selected from the UCM application. Models included in this series are the 8811, 8831, 8841, 8845, 8851, 8851 NR, 8861, 8865. There are 88XX Series Tempest hardened versions of these phones certified by similarity. These provide security protections compliant with CNSSI 5001 for use in SCIF, and SAPF environments.

Cisco Webex Devices – The Webex endpoints are video enabled IP phones and are programmed from the UCM Cluster PEI devices, and the features are selected for the individual user from the UCM application.

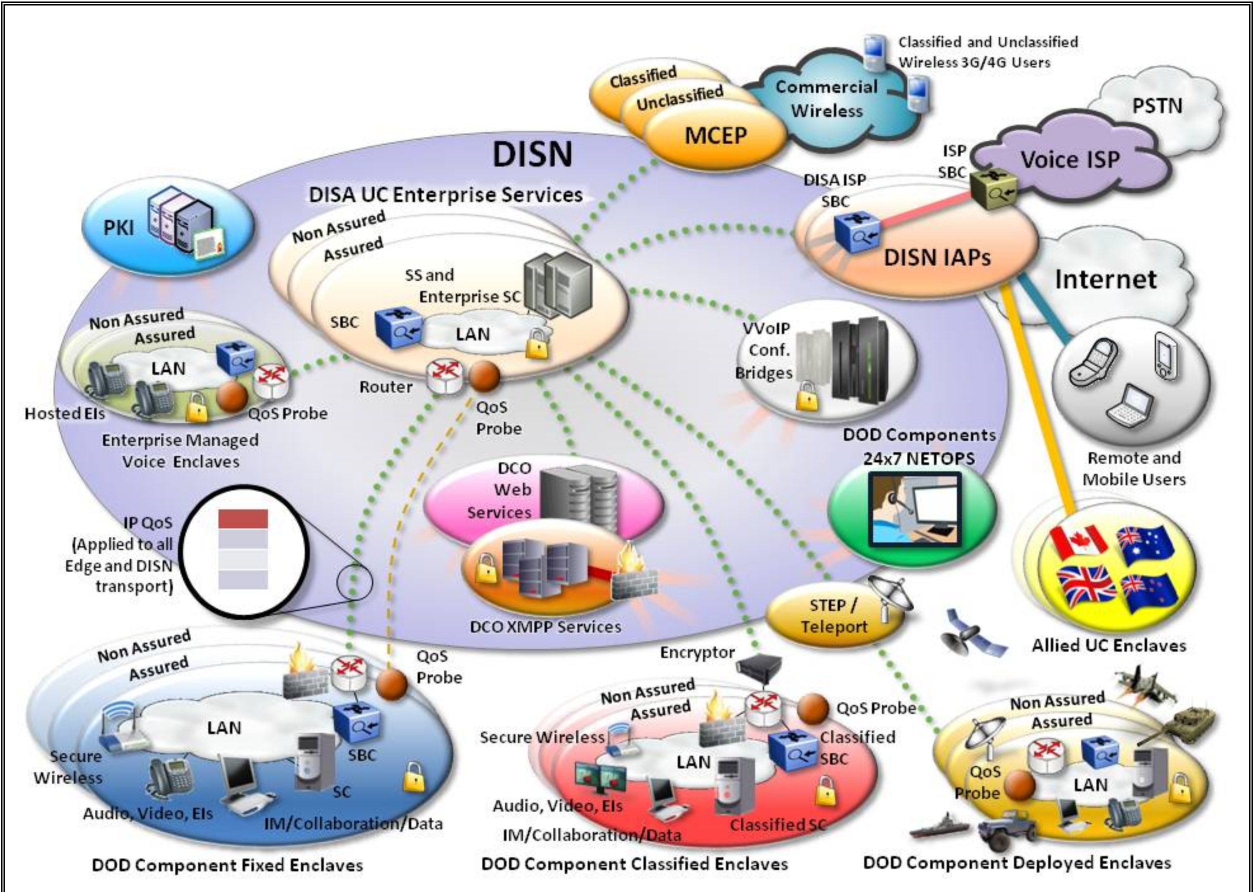
IP Phones 78XX Series – The 7811, 7821, 7841, and 7861 IP phones are programmed from the UCM Cluster as PEIs, and the features are selected for the individual user from the UCM application.

Cisco Jabber for Windows Client – Provides the main workspace application for the ESC. It enhances productivity by unifying presence, IM, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one client on a user's desktop. Cisco Jabber for Windows delivers highly secure, clear, and reliable communications. It offers flexible deployment models, is built on open standards, and integrates with commonly used desktop applications. The Cisco Jabber client can also connect remotely to the ESC 21 through the Cisco Expressway Advanced Collaboration GW.

3. OPERATIONAL ARCHITECTURE. The DoD Information Network (DoDIN) architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The DoD Chief Information Officer and Joint Staff policy and subscriber mission requirements determine the type of switch allowable at a particular location. The DoDIN architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational DoDIN architecture in which the SUT may be used. Figure 2-2 depicts the Enterprise Unified Capabilities Services architecture. Figure 2-3 depicts the LSC functional model.

4. TEST CONFIGURATION. The Joint Interoperability Test Command (JITC) test team tested the SUT at JITC, Fort Huachuca, Arizona, in a manner and configuration similar to that of a notional operational environment. The test team conducted testing of the system's required functions and features using the test configurations depicted in Figures 2-4 through 2-8. Figure 2-4 depicts the SUT ESC Head End test configuration. Figure 2-5 depicts the Type 1 Environment test configuration. Figure 2-6 depicts the SUT Type 2 Environment test configuration. Figure 2-7 depicts the SUT Type 3 Environment test configuration. Figure 2-8 depicts the SUT Expressway/Mobile and Remote Access (MRA) test configuration. Cybersecurity (CS) testing used the same configuration.

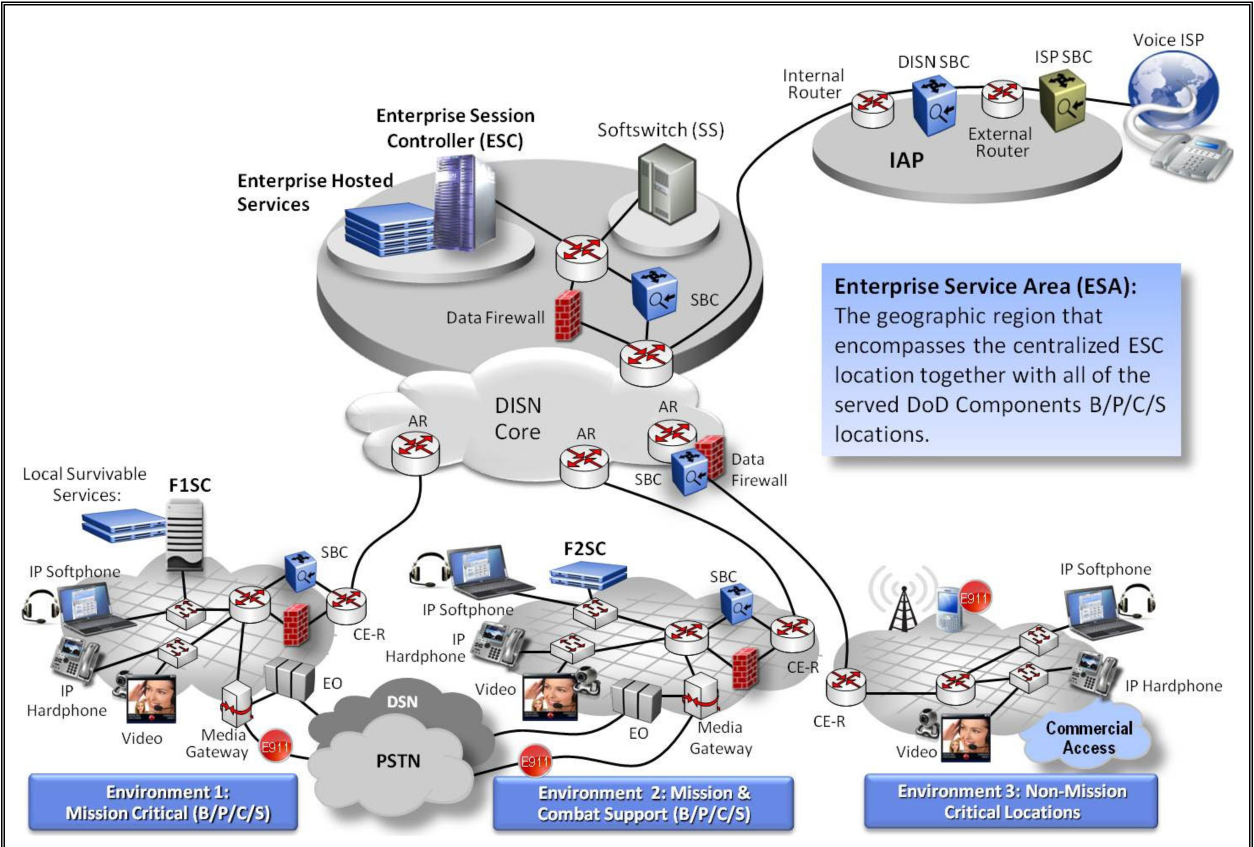
5. METHODOLOGY. The JITC test team conducted testing using ESC requirements derived from the Unified Capabilities Requirements (UCR) 2013, Change 2, Reference (b), and ESC test procedures, Reference (c). In addition to testing, an analysis of the Vendor's Letters of Compliance (LoC) verified the SUT met letter "R" requirements. Test Discrepancy Reports (TDRs) document any noted discrepancies. The Vendor submitted Plan of Action and Milestones (POA&M) as required. The Defense Information Systems Agency (DISA) adjudicated the TDRs as minor. DISA will evaluate any new discrepancy noted in the operational environment for impact on the existing certification. DISA will adjudicate these discrepancies via a vendor POA&M, which will address all new critical 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
DoDIN	DoD Information Network	SBC	Session Border Controller
EI	End Instrument	SC	Session Controller
IAP	Internet Access Point	SS	Softswitch
IM	Instant Messaging	STEP	Standardized Tactical Entry Point
IP	Internet Protocol	UC	Unified Capabilities
ISP	Internet Service Provider	VVoIP	Voice and Video over IP
LAN	Local Area Network	XMPP	Extensible Messaging and Presence Protocol
MCEP	Multi Carrier Entry Point		

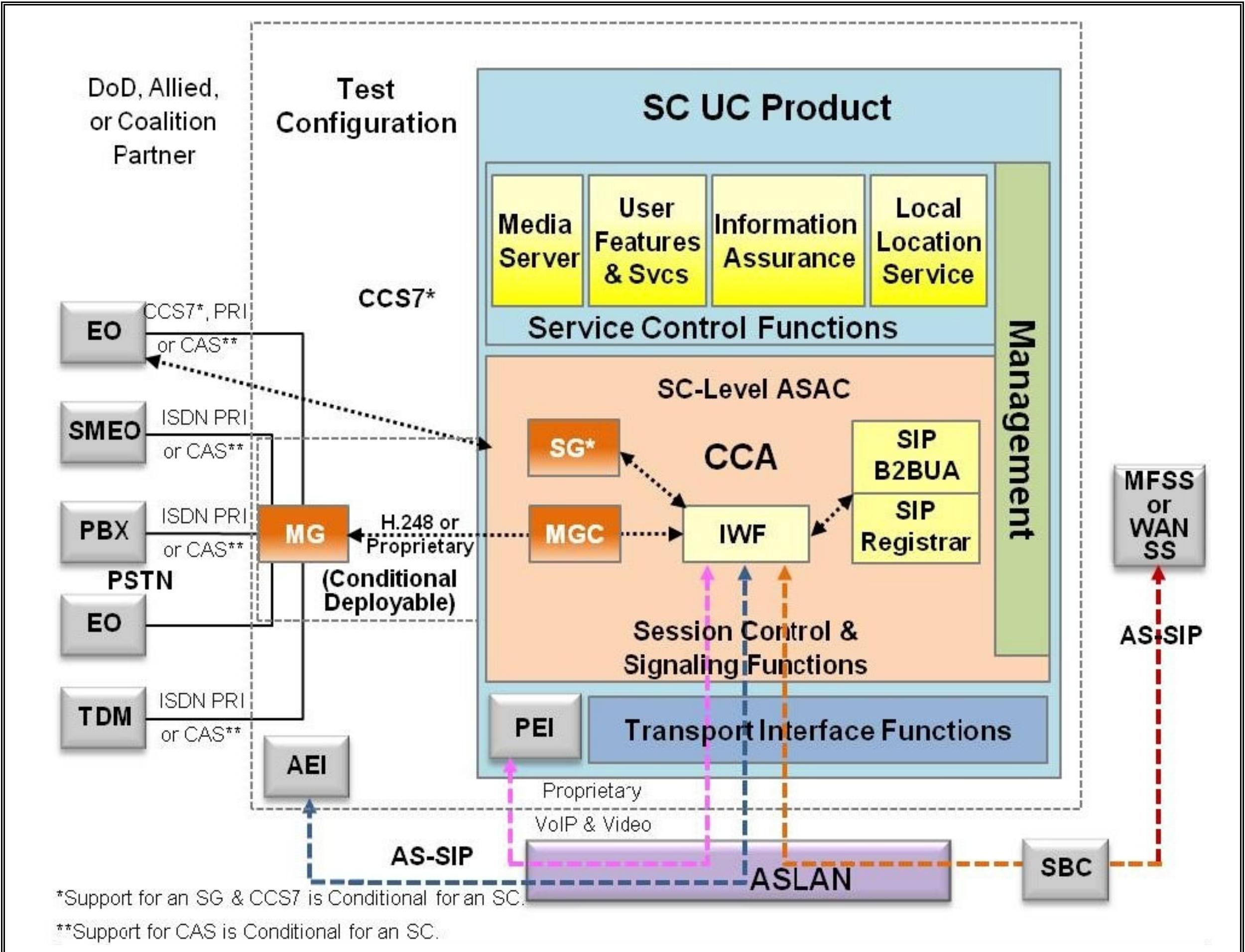
Figure 2-1. Notional DoDIN Architecture



LEGEND:

AR	Aggregation Router	F1SC	Failover Type 1 Session Controller
B/P/C/S	Base/Post/Camp/Station	F2SC	Failover Type 2 Session Controller
CE-R	Customer Edge Router	IAP	Internet Access Point
DISN	Defense Information Systems Network	IP	Internet Protocol
DoD	Department of Defense	ISP	Internet Service Provider
DSN	Defense Switched Network	PSTN	Public Switched Telephone Network
EO	End Office	SBC	Session Border Controller
ESA	Enterprise Service Area	SS	Softswitch
ESC	Enterprise Session Controller		

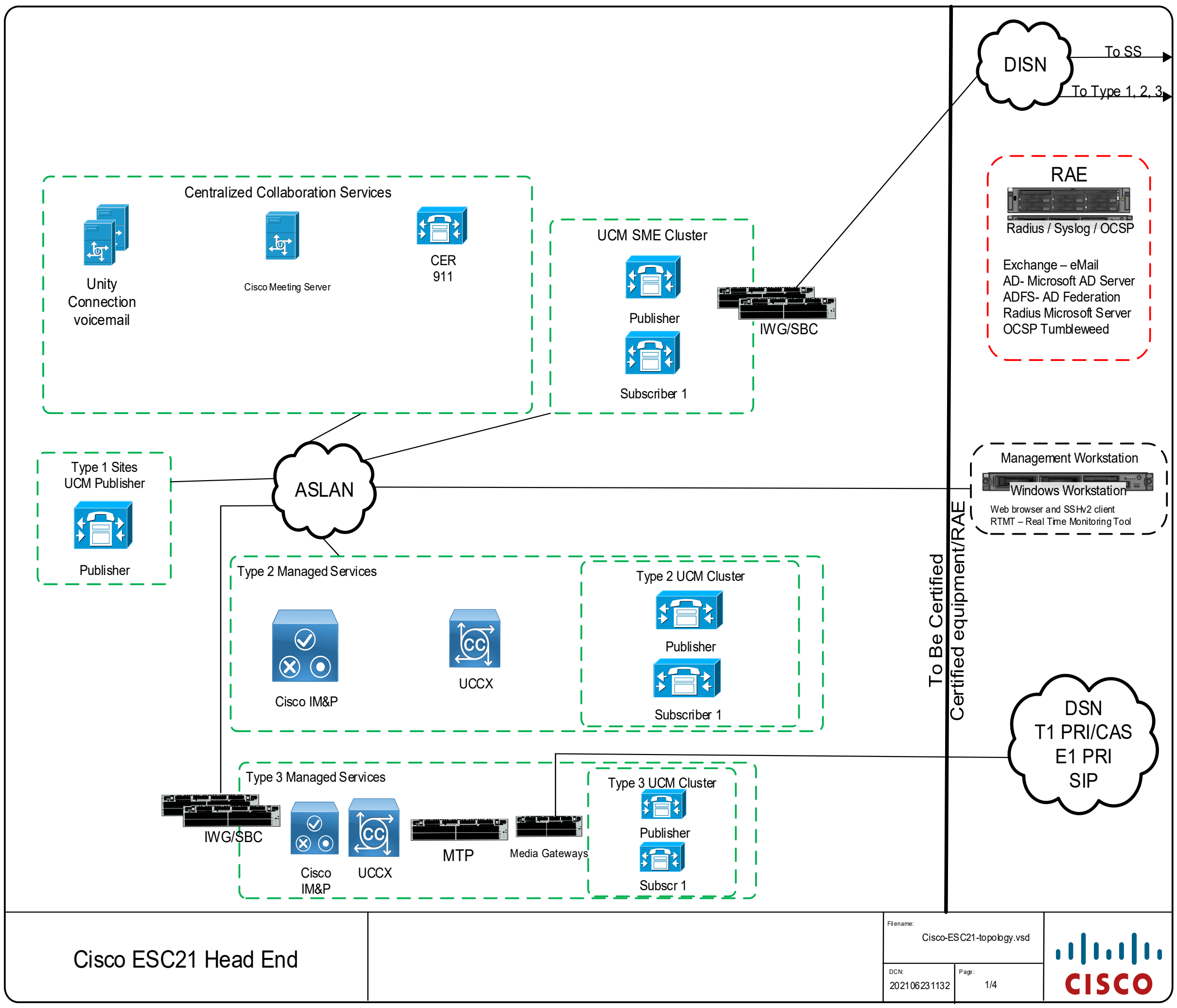
Figure 2-2. Enterprise Unified Capabilities Services Architecture



LEGEND:

AEI	AS-SIP End Instrument	PBX	Private Branch Exchange
ASAC	Assured Services Admission Control	PEI	Proprietary End Instrument
ASLAN	Assured Services Local Area Network	PRI	Primary Rate Interface
AS-SIP	Assured Services Session Initiation Protocol	PSTN	Public Switched Telephone Network
B2BUA	Back-to-Back User Agent	SBC	Session Border Controller
CAS	Channel Associated Signaling	SC	Session Controller
CCA	Call Connection Agent	SG	Signaling Gateway
CCS7	Common Channel Signaling 7	SIP	Session Initiation Protocol
DoD	Department of Defense	SMEO	Small End Office
EO	End Office	SS	Softswitch
ISDN	Integrated Services Digital Network	Svcs	Services
IWF	Interworking Function	TDM	Time Division Multiplexing
LSC	Local Session Controller	UC	Unified Capabilities
MFSS	Multifunction Softswitch	VoIP	Voice over Internet Protocol
MG	Media Gateway	WAN	Wide Area Network
MGC	Media Gateway Controller		

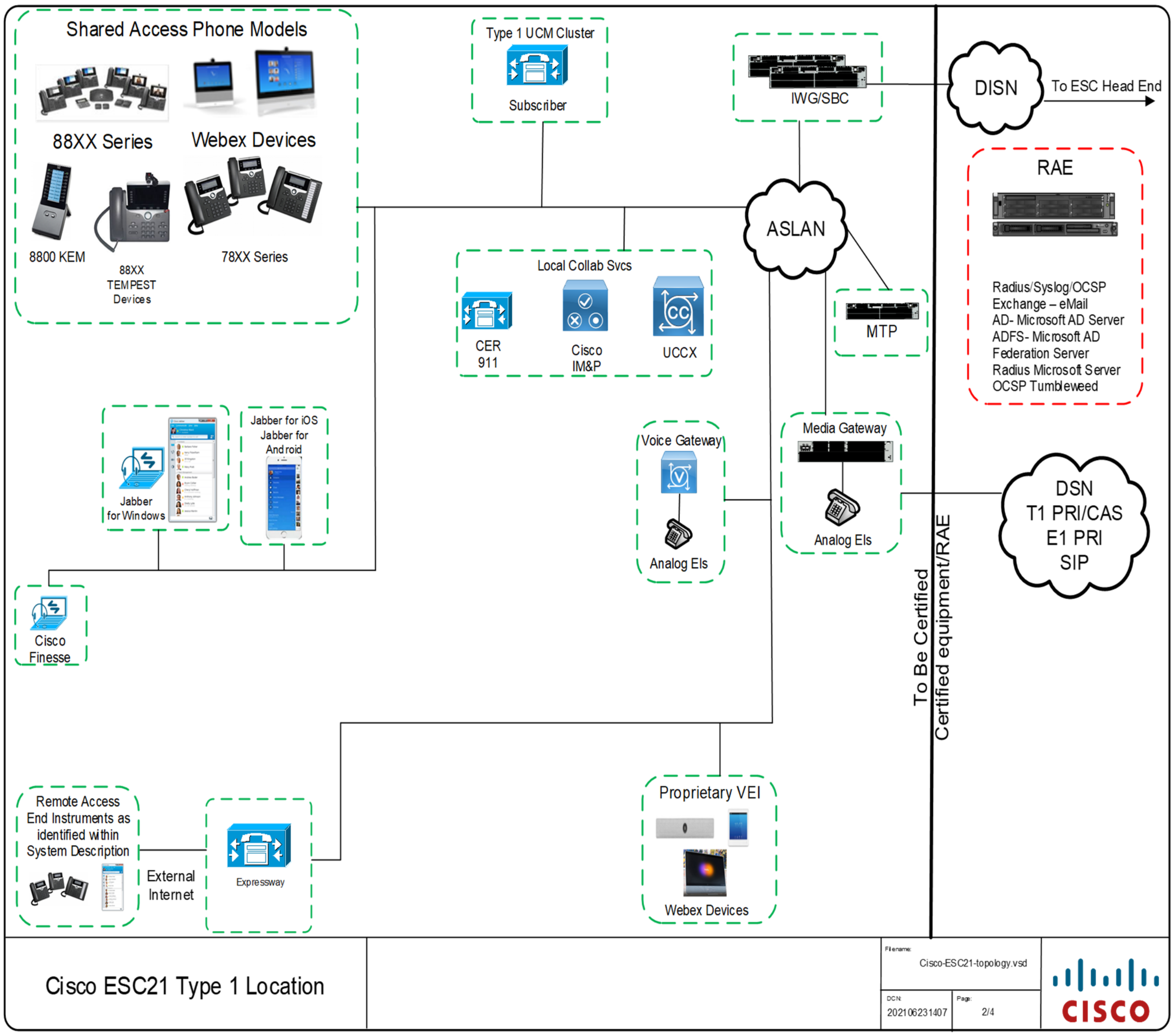
Figure 2-3. LSC Functional Reference Model



LEGEND:

AD	Active Directory	PRI	Primary Rate Interface
ADFS	Active Directory Federation Services	RADIUS	Remote Authentication Dial-In User Service
ASLAN	Assured Services Local Area Network	RAE	Required Ancillary Equipment
CAS	Channel Associated Signaling	RTMT	Real Time Monitoring Test
CER	Cisco Emergency Responder	SBC	Session Boarder Controller
DISN	Defense Information Systems Network	SIP	Session Initiation Protocol
DSN	Defense Switched Network	SME	Session Management Edition
E1	European Basic Multiplex Rate (2.048 Mbps)	SS	Softswitch
ESC	Enterprise Session Controller	SSHv2	Secure Shell version 2
IM&P	Instant Messaging & Presence	SUT	System Under Test
IWG	Interworking Gateway	Syslog	System log
Mbps	Megabits per second	T1	Digital Transmission Link Level 1 (1.544 Mbps)
MTP	Media Termination Point	UCCX	Unified Contact Center Express
OCSP	Online Certification Status Protocol	UCM	Unified Communications Manager

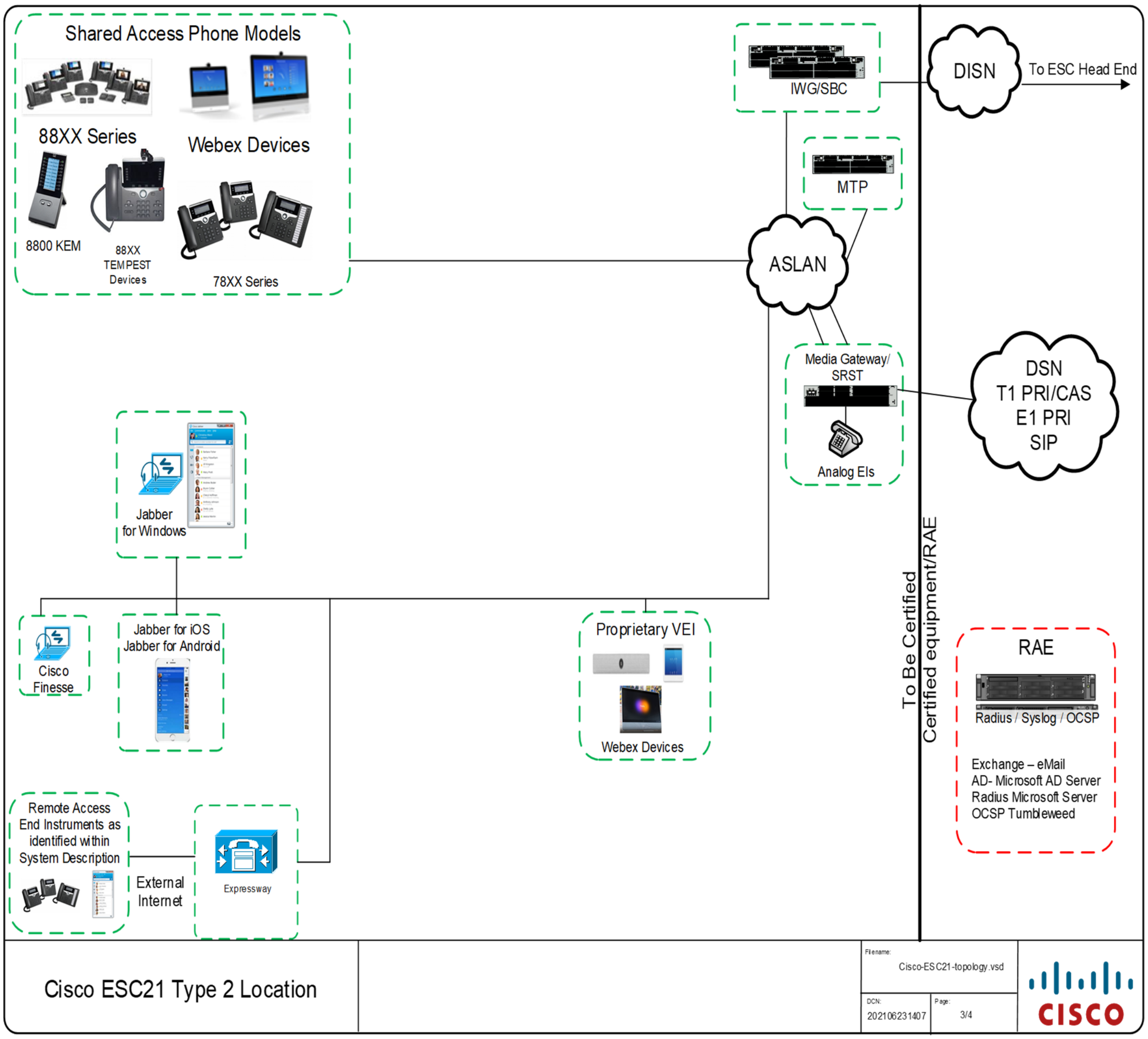
Figure 2-4. SUT ESC Head End Test Configuration



LEGEND:

AD	Active Directory	Mbps	Megabits per second
ADFS	Active Directory Federation Services	MTP	Media Termination Point
ASLAN	Assured Services Local Area Network	OCSP	Online Certification Status Protocol
CAS	Channel Associated Signaling	PRI	Primary Rate Interface
CER	Cisco Emergency Responder	RADIUS	Remote Authentication Dial-In User Service
DISN	Defense Information Systems Network	RAE	Required Ancillary Equipment
DSN	Defense Switched Network	SBC	Session Boarder Controller
E1	European Basic Multiplex Rate (2.048 Mbps)	SIP	Session Initiation Protocol
EI	End Instrument	SUT	System Under Test
ESC	Enterprise Session Controller	Syslog	System log
IM&P	Instant Messaging & Presence	T1	Digital Transmission Link Level 1 (1.544 Mbps)
iOS	iPhone Operating System	UCCX	Unified Contact Center Express
IWG	Interworking Gateway	UCM	Unified Communications Manager
KEM	Key Expansion Module	VEI	Video End Instruments

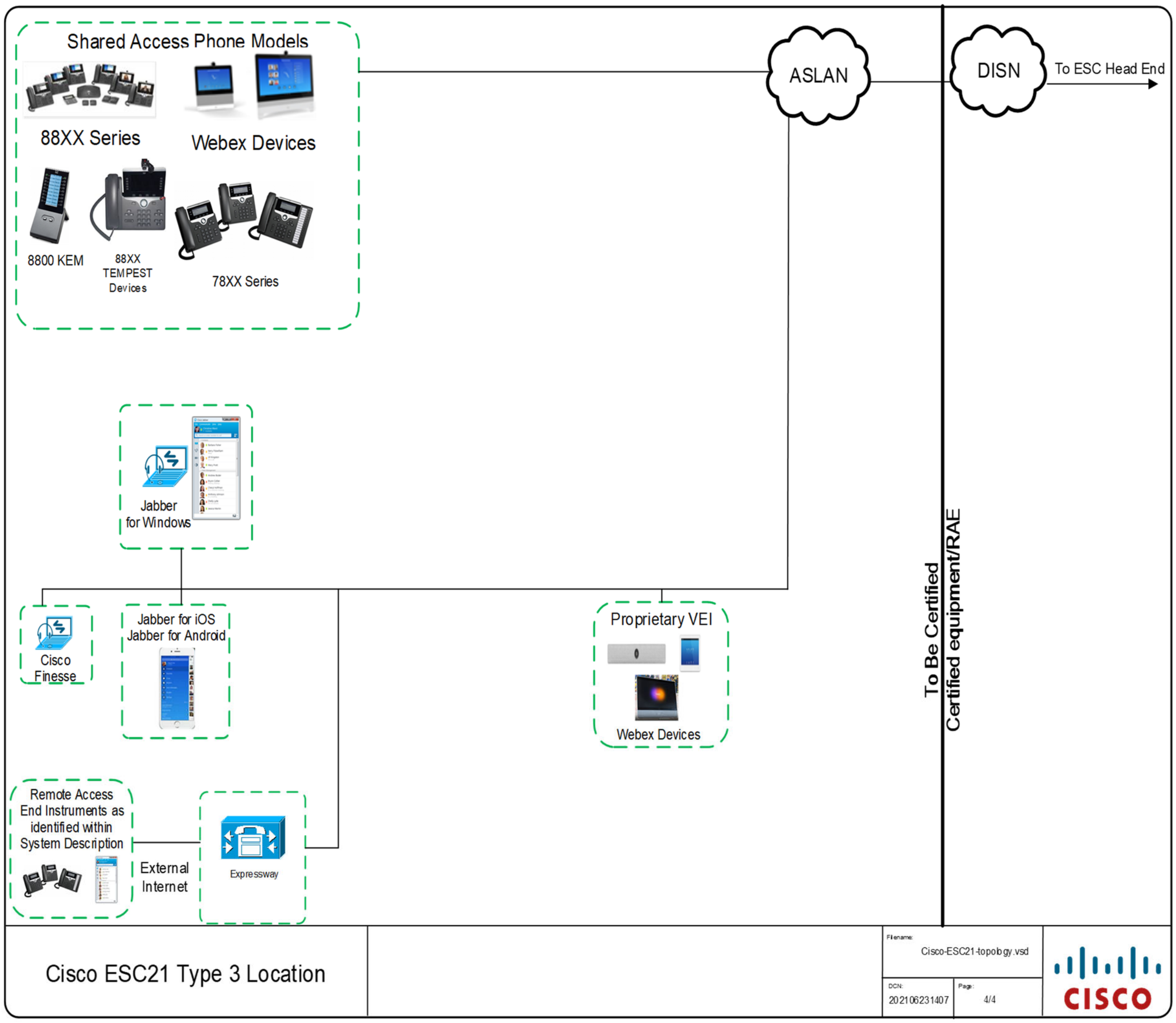
Figure 2-5. SUT Type 1 Environment Test Configuration



LEGEND:

AD	Active Directory	MTP	Media Terminal Point
ASLAN	Assured Services Local Area Network	OCSP	Online Certificate Status Protocol
CAS	Channel Associated Signaling	PRI	Primary Rate Interface
DISN	Defense Information Systems Network	RADIUS	Remote Authentication Dial-In User Service
DSN	Defense Switch Network	RAE	Required Ancillary Equipment
E1	European Basic Multiplex Rate (2.048 Mbps)	SBC	Session Boarder Controller
EI	End Instrument	SIP	Session Initiation Protocol
ESC	Enterprise Session Controller	SRST	Survivable Remote Site Telephony
iOS	iPhone Operating System	SUT	System Under Test
IWG	Interworking Gateway	Syslog	System log
KEM	Key Expansion Module	T1	Digital Transmission Link Level 1 (1.544 Mbps)
Mbps	Megabits per second	VEI	Video End Instruments

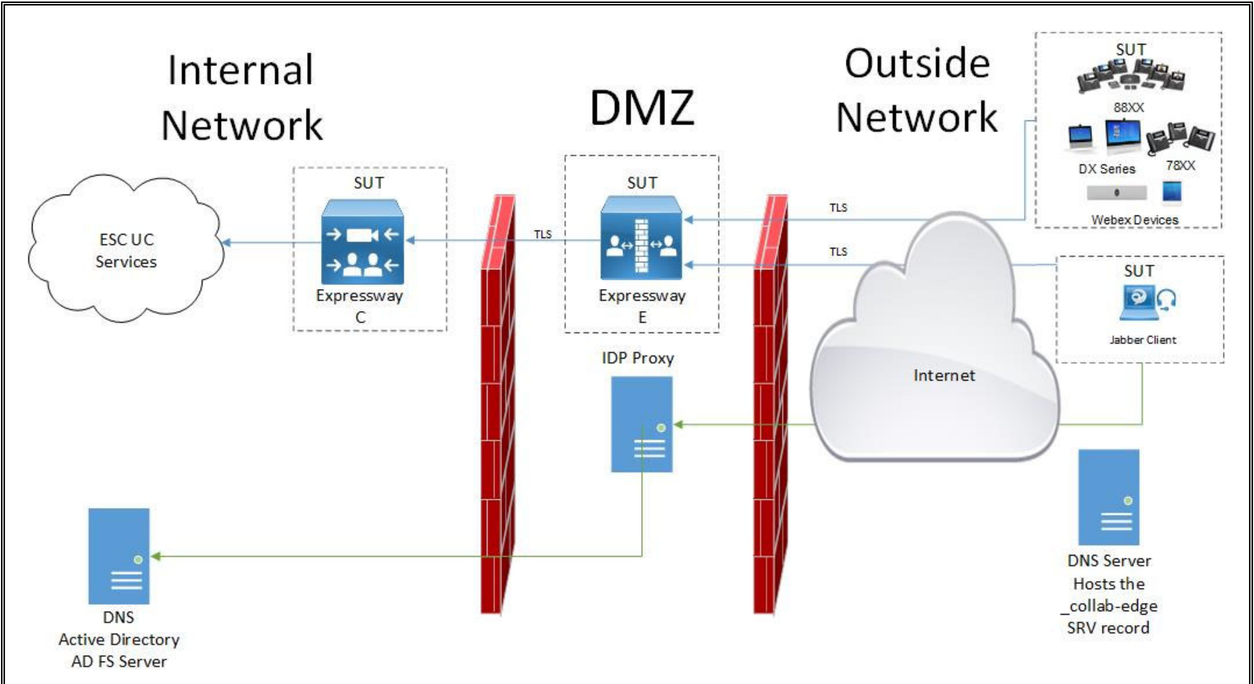
Figure 2-6. SUT Type 2 Environment Test Configuration



LEGEND:

ASLAN	Assured Services Local Area Network	KEM	Key Expansion Module
DISN	Defense Information Systems Network	RAE	Required Ancillary Equipment
ESC	Enterprise Session Controller	SUT	System Under Test
iOS	iPhone Operating System	VEI	Video End Instrument

Figure 2-7. SUT Type 3 Environment Test Configuration



LEGEND:

AD FS	Active Directory Federal Services	MRA	Mobile and Remote Access
DNS	Domain Name System	SRV	Service
DMZ	Demilitarized Zone	SUT	System Under Test
ESC	Enterprise Session Controller	TLS	Transport Layer Security
IDP	Identity Provider	UC	Unified Capabilities

Figure 2-8. SUT Expressway/MRA Test Configuration

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The interface, Capability Requirements (CR) and Functional Requirements (FR), CS, and other requirements for Session Controllers (SCs) are defined by UCR 2013, Change 2, Sections 2, 4, and 5. Table 3-1 provides the SUT interface interoperability status, and Table 3-2 provides the CR and FR status. Testing details and results are provided in the subparagraphs below. Optional and/or conditional requirements are not included in the test results unless otherwise noted.

a. Interface Status. The interface requirements are established in the UCR 2013, Change 2, Section 2.7, and Table 3-1 provides the SUT interface interoperability status.

b. The UCR 2013, Change 2, section 2.2, includes the requirements for Voice Features and Capabilities in the subparagraphs below.

1) The UCR 2013, Change 2, Section 2.2, states that it is expected that all Assured Services products, such as SCs and Softswitches (SSs), will support vendor-proprietary Voice and Video over IP (VVoIP) features and capabilities. The product's support for these vendor-proprietary VVoIP features and capabilities shall not adversely affect the required operation of the Multi-Level Precedence and Preemption (MLPP) or Assured Services Admission Control (ASAC) features on that product. The SUT met this requirement with testing and the Vendor's LoC. In addition, the LSC shall meet the requirements in the subparagraphs below.

2) The UCR 2013, Change 2, Section 2.2.1, includes four types of call forwarding features considered for UC: Call Forwarding Variable (CFV), Call Forwarding Busy Line (CFBL), Call Forwarding - Don't Answer - All Calls (CFDA), and Selective Call Forwarding (SCF). Call forwarding interaction with MLPP and a reminder ring for call forwarding features are optional. The SUT met this requirement with testing and the Vendor's LoC.

3) The UCR 2013, Change 2, Section 2.2.2, includes the requirements for MLPP Interactions with Call Forwarding (CF). If a call is forwarded by a CF feature that supports MLPP, the precedence level of the call shall be preserved during the forwarding process. This section includes the following features: Call Forwarding at a Busy Station and Call Forwarding - No Reply at Called Station. The SUT met this requirement with testing.

4) The UCR 2013, Change 2, Section 2.2.3, includes the requirements for Precedence Call Waiting. The following treatments apply to precedence levels of PRIORITY and above: Busy With Higher Precedence Call, Busy With Equal Precedence Call, No Answer, Line Active With a Lower Precedence Call, and Call Waiting for Single Call Appearance VoIP Phones. The SUT met these requirements with testing and the Vendor's LoC.

5) The UCR 2013, Change 2, Section 2.2.4, includes the requirements for Call Transfer. The two types of call transfers are normal and explicit. A normal call transfer is a transfer of an incoming call to another party. An explicit call transfer happens when both calls are originated by the same subscriber. This section includes the following features: Call Transfer Interaction at Different Precedence Levels and Call Transfer Interaction at Same Precedence Levels. The SUT met these requirements with testing.

6) The UCR 2013, Change 2, Section 2.2.5, Call Hold, states that the calls on hold shall retain the precedence of the originating call. The SUT met this requirement with testing.

7) The UCR 2013, Change 2, Section 2.2.6, includes the requirements for Three-Way Calling (TWC). The SUT met these requirements with testing and the Vendor's LoC.

8) The UCR 2013, Change 2, Section 2.2.7, includes the requirements for Hotline Service. This requirement was not tested but was determined by JITC analysis to be compliant based upon previous test data collected on the same hardware platform with similar performing software, and product maturity.

9) The UCR 2013, Change 2, Section 2.2.8, includes the requirements for Calling Number Delivery. The SUT met these requirements with testing and the Vendor's LoC.

10) The UCR 2013, Change 2, Section 2.2.9, includes the requirements for Call Pick-Up. This requirement was not tested but was determined by JITC analysis to be compliant based upon previous test data collected on the same hardware platform with similar performing software, and product maturity.

11) The UCR 2013, Change 2, Section 2.2.10, includes the requirements for Precedence Call Diversion. The SUT met these requirements with testing and the Vendor's LoC.

12) The UCR 2013, Change 2, Section 2.2.11, includes the requirements for Public Safety Voice Features. This section includes the following features: Basic Emergency Service (911), Tracing of Terminating Calls, Outgoing Call Tracing, Tracing of a Call in Progress, and Tandem Call Trace. The SUT met these requirements with testing and the Vendor's LoC.

c. The UCR 2013, Change 2, Section 2.3, includes the requirements for ASAC in the subparagraphs below.

1) The UCR 2013, Change 2, Section 2.3.1, includes the requirements for ASAC requirements related to voice. This section includes the following requirements: Voice Session Budget Unit, ASAC States, Session Control Processing with No Directionalization, and SC Session Control Processing with Directionalization. The SUT met these requirements with testing with No Directionalization (Total Count). The SUT does not support the optional ASAC with Directionalization.

2) The UCR 2013, Change 2, Section 2.3.3, includes the requirements for ASAC Requirements for the SC and the SS Related to Video Services. The SUT met these requirements with testing with No Directionalization. The SUT does not support the optional ASAC with Directionalization.

d. The UCR 2013, Change 2, Section 2.4, includes the requirements for Signaling Protocols. This section also includes the Signaling Performance Guidelines, which include call setup and call tear-down times as well as guidelines for intra-enclave, inter-enclave and worldwide calls. The SUT met these requirements with testing and the Vendor's LoC.

e. The UCR 2013, Change 2, Section 2.5, includes the requirements for Registration and Authentication. Registration and authentication between Network Elements (NEs) shall follow the requirements set forth in Section 4, Cybersecurity. This section includes additional Network Time Protocol (NTP) requirements. The JITC-led CS test team completed security testing and published the results in a separate report, Reference (d).

f. The UCR 2013, Change 2, Section 2.6, includes the requirements for SC and SS Failover and Recovery. An SC may be provisioned with direct links to any number of other SCs (i.e., direct tertiary routes) and provisioned with the set of addresses or record served by each SC with which it has a direct tertiary route. Each SC and SBC pairing shall support OPTIONS-based failover by at least one of the following methods under UCR 2013, Change 2, Sections 2.6.1 or 2.6.2.

1) Section 2.6.1, SC Failover: Alternative A: The SC-Generated OPTIONS Method. This section covers SC-Generated OPTIONS, SC OPTIONS-based Failover, SC-based Failback and Failure Handling for Outbound Dialog-initiating INVITE. The SUT does not support this failover alternative.

2) Section 2.6.2, SC Failover: Alternative B: The SBC-Generated OPTIONS Method. This section covers SBC-Generated OPTIONS, SBC-based Failover, SBC-based Failback and Failure Handling for Outbound Dialog-initiating INVITE. The SUT met this requirement with testing.

g. The UCR 2013, Change 2, Section 2.7, includes the requirements for Product Interfaces. This includes requirements for internal and external physical interfaces, interfaces to other networks, and DISA VVoIP Element Management System (EMS) Interface.

1) The UCR 2013, Change 2, Section 2.7.1, states that internal interfaces are functions that operate internal to an SUT or UC-approved product (e.g., SC, SS). The interfaces between SC/SS functions within an SC and Signaling Gateway (SG) are considered internal to the SC regardless of the physical packaging. These interfaces are vendor-proprietary and unique, especially the protocol used over the interface. Whenever the physical interfaces use Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

2) The UCR 2013, Change 2, Section 2.7.2, states External Physical Interfaces Between Network Components are functions that cross the demarcation point between SUT and other external network components. Whenever the physical interfaces use IEEE 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard

802.3ab, 1999. This requirement does not preclude the use of other types of physical interfaces. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

a) The SC (and its appliances), SS, SBC, Assured Services Session Initiation Protocol (AS-SIP) EI (AEI), and PEI shall support one or more of the following Ethernet physical interfaces (compliant to IEEE 802.3 standards) to Assured Services Local Area Network (ASLAN) switches and routers. The SUT met this requirement with testing and the Vendor's LoC.

b) If the physical interface supports multiple Ethernet rates, it shall support auto-negotiation. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

3) The UCR 2013, Change 2, Section 2.7.3, states that interfaces to other networks, are interfaces where traffic flows from one network (e.g., UC) to another network (e.g., Public Switched Telephone Network (PSTN)). The SUT met this requirement with testing and the Vendor's LoC.

a) The Deployable interface requirements are specified in Appendix A, Unique Deployed (Tactical), and Section 6, Network Infrastructure End-to-End Performance. These requirements are unique optional requirements for a deployed SC and were not tested.

b) The Assured Services subsystem shall interface the Teleport sites on both a TDM basis and an IP basis. An American National Standards Institute (ANSI) T1.619a (Signaling System 7 and Integrated Services Digital Network (ISDN) MLPP Signaling Standard for T1) MG with Primary Rate Interface (PRI) signaling will be used for T1 trunks to the Teleport sites. If the Teleport site contains an SC, then the interface will be via the DISN wide area network (WAN) for both the media and signaling, with the signaling being AS-SIP (AS-SIP 2013) between the Teleport SC and the UC SS. The SUT met this requirement with testing and the Vendor's LoC.

c) The Assured Services subsystem shall interface with the PSTN and host-nation via the MG interfaces as specified in Section 2.16, Media Gateway. The SUT met this requirement with testing and the Vendor's LoC.

d) Voice and video interfaces with allied and coalition networks have not yet been defined. Therefore, the interface will remain TDM as specified in UCR 2013, Figure 4.4.2-1, Defense Switched Network (DSN) Design and Components.

4) The UCR 2013, Change 2, Section 2.7.4, states that SCs shall support a 10/100-Mbps Ethernet physical interface to the DISA VVoIP EMS. The interface will work in either of the two following modes using auto-negotiation: IEEE, Ethernet Standard 802.3, 1993; or IEEE,

Fast Ethernet Standard 802.3u, 1995. The SUT met this requirement with testing and the Vendor's LoC.

h. The UCR 2013, Change 2, Section 2.8, includes the requirements for the Product Physical, Quality and Environmental Factors.

1) The UCR 2013, Change 2, section 2.8.2.1, includes the Product Availability requirements. This includes requirements for the following three availability options: High Availability, Medium Availability, and Medium Availability for non-Command and Control (C2) users. However, an ESC must meet the High Availability requirements. The SUT met the requirements for High Availability ESC with testing and the Vendor's LoC.

a) High Availability. The Assured Services appliance shall have a hardware or software availability of 99.999 percent (a non-availability state of no more than 5 minutes per year). The vendor shall provide an availability model for the appliance showing all calculations and showing how the overall availability will be met. The subsystem(s) shall have no single point of failure that can cause an outage of more than 96 voice and/or video subscribers. To meet the availability requirements, all subsystem(s) platforms that offer service to more than 96 voice and/or video subscribers shall have a modular chassis that provides, at a minimum, the following: Dual Power Supplies, Dual Processors/Swappable Sparing (Control Supervisors), Termination Sparing, Redundancy Protocol, No Single Failure Point, Switch Fabric or Backplane Redundancy for Active Backplanes, Software Upgrades and Patches, Backup Power UPS Requirements, No Loss of Active Sessions. In addition, when an appliance component fails and the backup component takes over, each media stream for each active call shall remain active during the failover, until either 1) timer expirations or lack of state information cause that call to terminate or 2) the EI subscribers on that call, naturally terminate the call. The SUT met these requirements with testing and the Vendor's LoC.

b) Medium Availability. The Medium Availability SC shall have a hardware or software availability of 99.99 percent (a non-availability state of no more than 53 minutes per year). The vendor shall provide an availability model for the appliance showing all calculations and showing how the overall availability will be met. In support of the availability requirements, all subsystem(s) platforms that offer service to more than 96 voice and/or video subscribers shall have a modular design and chassis that provides, at a minimum, the following: Dual Power Supplies, Software Upgrades and Patches, No Loss of Active Sessions. In addition, when an Appliance component fails and the backup component takes over, each media stream for each active call shall remain active during the failover, until either 1) timer expirations or lack of state information causes that call to terminate or 2) the EI subscribers on that call naturally terminate the call. The SUT by virtue of meeting the High Availability requirements also meets these lesser Medium Availability requirements.

c) Medium Availability not for Special C2 users. The Medium Availability SC shall have a modular design and chassis that provides, at a minimum, the following: Dual Processors/Swappable Sparing (Control Supervisors), Termination Sparing, Redundancy Protocol, No Single Failure Point, Switch Fabric or Backplane Redundancy for Active

Backplanes, and Backup Power UPS Requirements. The SUT by virtue of meeting the High Availability requirements also meets this lesser Medium Availability requirement.

2) The UCR 2013, Change 2, Section 2.8.2.2, includes the Maximum Downtime requirements. This includes requirements for the following products: High Availability and Medium Availability. The SUT by virtue of meeting the High Availability requirements also meets these lesser Medium Availability requirements.

a) High Availability. The performance parameters associated with the ASLAN, SS, and High Availability SC, when combined, shall meet the following maximum downtime requirements: IP (10/100/1000 Ethernet) network links - 35 minutes per year and IP subscriber - 12 minutes per year. The SUT met this requirement with the Vendor's LoC.

b) Medium Availability. The performance parameters associated with the ASLAN, SS, and Medium Availability SC, when combined, shall meet the following maximum downtime requirements: IP (10/100/1000 Ethernet) network links - 82 minutes per year and IP subscriber – 60 minutes per year. The SUT met this requirement with the Vendor's LoC.

3) The UCR 2013, Change 2, Section 2.8.4, states that, for the VoIP devices, the voice quality shall have a Mean Opinion Score (MOS) of 4.0 (R-Factor equals 80) or better, as measured in accordance with (IAW) the E-Model. Additionally, these devices shall not lose two or more consecutive packets in a minute and shall not lose more than seven voice packets (excluding signaling packets) in a 5-minute period. This applies only to devices that generate media and have a Network Interface Card (NIC). The SUT met these requirements with testing with an average MOS score of 4.40.

i. The UCR 2013, Change 2, section 2.9, includes the requirements for EIs in the subparagraphs below.

1) The UCR 2013, Change 2, Section 2.9.1, includes the requirements for IP Voice EIs. This section includes the basic requirements, tones and announcements, audio codecs for voice instruments, VoIP telephone audio performance, VoIP sampling standard, softphones, and Differentiated Services Code Point (DSCP) packet marking. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

2) The UCR 2013, Change 2, Section 2.9.2, includes the requirements for analog and ISDN Basic Rate Interface (BRI) Telephone Support. The SUT does not support BRI but met the requirements for analog with testing and the Vendor's LoC.

3) The UCR 2013, Change 2, Section 2.9.3, includes the requirements for Video EIs. Video EIs are considered associated with the SC and must have designated in conjunction with the SC design. This section includes the basic requirements; display messages, tones, and announcements; video codecs including associated audio codecs; and H.323 video

teleconferencing. The SUT offers H.323 Video EIs; however, they were not tested and are not included in this certification.

4) The UCR 2013, Change 2, Section 2.9.4, states that the PEI and AEI shall each be capable of authenticating itself to its associated SC and vice versa IAW Section 4, Cybersecurity. The SUT met this requirement with the Vendor's LoC. In addition, the JITC-led CS test team conducted security testing and published the results in a separate report, Reference (d).

5) The UCR 2013, Change 2, Section 2.9.5, states that the EI interface to the ASLAN shall be IAW Ethernet (IEEE 802.3) Local Area Network (LAN) technology. The 10-Mbps and 100-Mbps Fast Ethernet (IEEE 802.3u) shall be supported. The SUT met this requirement with testing and the Vendor's LoC.

6) The UCR 2013, Change 2, Section 2.9.6, includes the requirements for Operational Framework for AEIs. This section contains SC and AS-SIP EI requirements to support a generic, multivendor-interoperable interface between a VVoIP SC and an AS-SIP VVoIP EI, which can be a voice EI, a secure voice EI, or a video EI. This generic, multivendor-interoperable interface uses AS-SIP protocol instead of the various vendor-proprietary SC-to-EI protocols. This section includes the following requirements: Requirements for Supporting AS-SIP EIs, Requirements for AS-SIP voice EIs, Requirements for AS-SIP Secure voice EIs, Requirements for AS-SIP video EIs, and AS-SIP video EI features. The SUT AEI signaling protocol was not tested because there were no AEIs submitted with the SUT. In addition, there are no AEIs on the DoDIN Approved Products List (APL) certified with the SUT. The SUT met these requirements with testing with the voice and video PEI interfaces only.

7) The UCR 2013, Change 2, Section 2.9.7, includes the requirements for Multiple Call Appearance Requirements for AS-SIP EIs. This section includes the following requirements: Multiple Call Appearance Scenarios, Multiple Call Appearances - Specific Requirements, and Multiple Call Appearances - Interactions with Precedence Calls. The SUT does not support AEI; however, the SUT met the requirement for multiple call appearances with the testing of their PEIs.

8) The UCR 2013, Change 2, Section 2.9.8 includes the requirements for PEIs, AEIs, Terminal Adapters, and Integrated Access Devices using the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Recommendation V.150.1 protocol. The SUT AEI signaling protocol was not tested because there were no AEIs submitted with the SUT. In addition, there are no AEIs on the DoDIN APL certified with the SUT. The SUT met these requirements with testing with the voice and video PEI interfaces only.

9) The UCR 2013, Change 2, Section 2.9.9 includes the requirements for UC Products with Non-Assured Service Features. The SUT does not support AEI; however, the SUT met the requirement for multiple call appearances with the testing of their PEIs.

10) The UCR 2013, Change 2, Section 2.9.10 includes the requirements for ROUTINE-Only EIs (ROEIs). SC support for ROEIs is optional; however, if they are supported the

requirements in this section apply. The SUT offers optional ROEIs; however, they were not tested and are not included in this certification.

j. The UCR 2013, Change 2, Section 2.10 includes the requirements for Session Controllers.

1) The UCR 2013, Change 2, Section 2.10.1, states the SC shall meet all the requirements for Precedence-Based Assured Services (PBAS) and ASAC, as appropriate for VoIP and Video over IP services, as specified in Section 2.25.1, Multilevel Precedence and Preemption and Section 2.3, ASAC. The SUT met this requirement with testing.

2) The UCR 2013, Change 2, Section 2.10.2 states the SC shall support AS-SIP over IP for signaling to AEIs and SSs. The SC shall optionally support AS-SIP over IP signaling to AEIs. The SC shall optionally support proprietary VVoIP signaling to interface with PEI. The SUT met the voice and video PEI signaling protocol requirements with testing and the Vendor's LoC.

3) The UCR 2013, Change 2, Section 2.10.3, states that the SC shall support a Session Controller Location Service (SCLS) functionality that provides information on call routing and called address translation. This requirement was not tested but was determined by JITC analysis to be compliant based on previous test data collected on the same hardware platform with similar performing software, and product maturity.

4) The UCR 2013, Change 2, Section 2.10.4, states that the SC shall support the applicable Fault, Configuration, Accounting, Performance, and Security (FCAPS) Management and Audit Log requirements specified in Section 2.19, Management of Network Appliances. The SUT met this requirement with the Vendor's LoC.

5) The UCR 2013, Change 2, Section 2.10.5, states that the SC shall provide an interface to the DISA VVoIP EMS. The interface consists of a 10/100-Mbps Ethernet connection as specified in Section 2.7.4, DISA VVoIP EMS Interface. The SUT met this requirement with testing and the Vendor's LoC.

6) The UCR 2013, Change 2, Section 2.10.6, states that the SC shall provide Transport Interface functions to interface with the ASLAN and its IP packet transport network. The SUT met this requirement with testing.

7) The UCR 2013, Change 2, Section 2.10.7, includes the requirements for Custom Line-Side Features Interference. If custom line-side features are implemented, they shall not interfere with the Assured Services requirements. The SUT does not support this optional requirement.

8) The UCR 2013, Change 2, Section 2.10.8, states that during the call establishment process, the product shall be capable of preventing or detecting and stopping hairpin routing loops over ANSI T1.619a and commercial PRI trunk groups between a legacy switch and an SC. The Loop Avoidance mechanism shall not block call requests that are legitimately redirected or

forwarded between the two interconnected products. In the event that a routing loop is detected, the SC shall clear the call in the backwards direction, either sending a 404 (Not Found) response to a SIP originator, or an ISDN DISCONNECT message (from the MG) to a TDM originator. The SC shall provide a Vacant Code Announcement to the caller in each case. This optional requirement was not tested but was determined by JITC analysis to be compliant based on previous test data collected on the same hardware platform with similar performing software, and product maturity.

9) The UCR 2013, Change 2, Section 2.10.9, states that the requirements in this section are unique to the distributed application for the Session Controller, the LSC. An LSC provides management for the EIs within a single B/P/C/S or enclave and is deployed at the same location as the EIs it serves. These requirements were not tested but were determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

10) The UCR 2013, Change 2, Section 2.10.9.1, states that in the event that total loss of connectivity to the DISN WAN occurs, the LSC shall provide the following functions: Completion of local calls (i.e., calls between EIs the LSC serves). Routing of calls to and from the PSTN, using a local MG (PRI or Channel Associated Signaling (CAS) as required by the local interface), that originate or terminate on EIs the LSC serves. User look-up of local directory information. The SUT met this requirement with testing and the Vendor's LoC.

k. The UCR 2013, Change 2, Section 2.11, includes requirements for the optional AS-SIP Gateways.

1) The UCR 2013, Change 2, Section 2.11.1, includes the optional requirements for the AS-SIP TDM Gateway Signaling. The SUT does not support this optional requirement.

2) The UCR 2013, Change 2, Section 2.11.2, includes requirements for the AS-SIP IP Gateway. The SUT does not support this optional requirement.

3) The UCR 2013, Change 2, Section 2.11.3, includes requirements for the AS-SIP – H.323 Gateway. The SUT does not support this optional requirement.

l. The UCR 2013, Change 2, Section 2.12, includes requirements for the Enterprise UC Services. The Enterprise UC Services Architecture consists of ESC Core Infrastructure products at a centralized "Master Site" location and Edge Infrastructure products at DoD Components' B/P/C/S locations. The ESC Core Infrastructure is composed of centralized ESC components, an ESC-fronting SBC, Enterprise Hosted UC Services and Enterprise RAE. The Edge Infrastructure consists of EIs, MGs, Enclave-fronting SBCs, local survivable call processing appliances (for Types 1 and 2) and local RAE. When the ESC is implemented in a distributed cluster configuration, individual ESC "cluster members" are deployed within the Edge Infrastructure at Type 1 and 2 Types (for further clarification, see Section 2.12.3.3.3). The centralized ESC Master Site, together with all of the served DoD Components' B/P/C/S locations, is collectively referred to as the Enterprise Services Area (ESA). These requirements apply to the SUT in an ESC configuration.

1) The UCR 2013, Change 2, Section 2.12.2.1, includes the ESC Core Infrastructure requirements in the subparagraphs below.

a) The UCR 2013, Change 2, Section 2.12.2.1.1, includes the general requirements in the subparagraphs below.

1. The ESC shall support the SC requirements defined in Section 2.10, Session Controller (subject to the modifications and additions set forth in this subsection). The SUT met this requirement with testing and the Vendor's LoC.

2. The ESC shall support centralized, integrated voice, video and data session management on behalf of served IP EIs that are located at different enclaves (i.e., B/P/C/S sites) within the associated ESA. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

3. The ESC shall be capable of autonomously providing session management for all intra-ESA voice and video sessions (where both the caller and called party reside within the ESA). The SUT met this requirement with testing and the Vendor's LoC.

4. The ESC shall be capable of interoperating with other ESCs and SCs using AS-SIP as defined in the AS-SIP 2013. The SUT met this requirement with testing and the Vendor's LoC. Refer to Table 3-4 for the list of SCs tested with the SUT.

5. Under normal operating conditions, the ESC shall rely upon the SS for all inter-ESA call routing. The SUT met this requirement with testing.

6. The ESC shall have an availability of at least 99.999%. The SUT met this requirement with the Vendor's LoC.

7. The ESC shall meet the IPv6 requirements defined in Section 5 of the UCR. The SUT met this requirement with testing and the Vendor's LoC.

8. The ESC shall support the DSCP marking requirements defined in Section 6, Network Infrastructure End-to-End Performance. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

9. Signaling, bearer, and Operations, Administration, Maintenance, and Provisioning (OAM&P) protocol traffic exchanged between the ESC Core infrastructure and the Edge infrastructure shall be capable of traversing DoD Component enclave and Enterprise cybersecurity accreditation boundaries using protocols that are approved by the Ports, Protocols, and Service Management (PPSM) Category Assurance List (CAL). The SUT met this requirement with the Vendor's LoC.

10. Each time an end user/EI registers for service with the ESC, the ESC shall determine the served enclave where the originating EI resides. This information shall permit the ESC to correctly associate a served enclave with every inbound (EI-to-ESC) or outbound (ESC-to-EI) call leg. Such an association is essential to the correct execution of services such as ASAC, Commercial Access, and Precedence Call Diversion. The precise mechanism for determining the enclave from which the registration request originated is left up to the vendor's discretion. The SUT met this requirement with the Vendor's LoC.

b) The UCR 2013, Change 2, Section 2.12.2.1.2, includes the support for EI requirements in the subparagraphs below.

1. The ESC shall support EI session management functions defined for the SC in Section 2.10, Session Controller (subject to the modifications and additions set forth in this subsection). The SUT met this requirement with testing and the Vendor's LoC.

2. The ESC shall offer hardware-based voice, video, and videophone EIs. The SUT met this requirement with testing and the Vendor's LoC.

3. The ESC shall offer soft clients that provide access to integrated UC services from a common user interface. In performing this function, the ESC shall comply with the softphone requirements defined in Section 2.9.1.6, Softphones. The SUT met this requirement with the Jabber client, which is certified as a voice and video softphone, and includes IM&P with XMPP as an XMPP client.

4. The ESC shall support an AS-SIP "ESC-to-EI" signaling interface in support of AEIs as defined in this section and the AS-SIP 2013. The ESC solution is not required to include AEIs. The SUT AEI signaling protocol was not tested because there were no AEIs submitted with the SUT. In addition, there are no AEIs on the DoDIN APL certified with the SUT. The SUT met these requirements with the voice and video PEI interfaces only.

5. If the ESC supports PEIs, then the vendor-proprietary "ESC-to-EI" signaling interface shall comply with the PEI signaling requirements as defined in Section 2.9.1, IP Voice End Instruments (subject to the modifications and additions set forth in this subsection). The SUT met this requirement with testing and the Vendor's LoC.

6. The ESC shall provide registrar functionality for all served EIs. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

c) The UCR 2013, Change 2, Section 2.12.2.1.3, includes the centralized configuration and OAM&P requirements in the subparagraphs below.

1. The ESC shall provide a centralized configuration service that permits served Edge Infrastructure products (EIs, MGs, SBCs, Failover Type 1 Session Controllers (F1SCs), Failover Type 2 Session Controllers (F2SCs), and distributed ESC cluster members) to securely

retrieve/download configuration files. The signaling and transport used to initiate and complete the retrieval and download of configuration files must be able to traverse DoD Component enclave and Enterprise cybersecurity accreditation boundaries using protocols that are approved by the PPSM CAL. The SUT met this requirement with the Vendor's LoC. The JITC-led CS test team completed security testing and published the results in a separate report, Reference (d).

2. The ESC shall enable centralized management and distribution of firmware/software updates directly to Edge Infrastructure products (including EIs, SBCs, MGs, F1SCs, F2SCs, and distributed ESC "cluster members"). The signaling and transport used to initiate and complete the distribution of firmware/software updates must be able to traverse DoD Component enclave and Enterprise cybersecurity accreditation boundaries using protocols that are approved by the PPSM CAL. The SUT met this requirement with the Vendor's LoC. The JITC-led CS test team completed security testing and published the results in a separate report, Reference (d).

3. The ESC vendor shall provide management solutions that enable the "centralized" provisioning, administration, management, accounting and monitoring of all ESC Cor Infrastructure components (i.e., including the centralized ESC, ESC-fronting SBC, and Enterprise Hosted UC Services) and all Edge Infrastructure components within the ESA (including EIs, Enclave-fronting SBCs, MGs, F1SCs, F2SCs, and distributed ESC "cluster members"). The SUT met this requirement with the Vendor's LoC.

4. The ESC shall permit local enclave administrators at served B/P/C/S locations to have secure, restricted access to the provisioning capabilities of the ESC for the purpose of provisioning local moves, adds and changes (MACs). Enclave administrative access privileges to the ESC's centralized provisioning capabilities shall be restricted to the extent that the local administrators can see and make only the provisioning changes that affect their local user community. The SUT met this requirement with the Vendor's LoC. The JITC-led CS test team completed security testing and published the results in a separate report, Reference (d).

d) The UCR 2013, Change 2, Section 2.12.2.1.4, includes the commercial access requirements in the subparagraphs below.

1. The ESC shall centrally provide MG Controller (MGC) functionality as defined in this section. In performing this function, the ESC shall be capable of routing commercial calls to an MG that resides in the same local enclave as the call originator. In the execution of this capability, the ESC shall leverage end user/EI-to-enclave association data determined at the time of end user/EI registration as described in Section 2.12.2.1.1. The SUT met this requirement with testing and the Vendor's LoC.

2. The ESC shall be capable of using AS-SIP to route commercial calls to the SS. To disambiguate an E.164 telephony number from a 10-digit DSN number within the AS-SIP Request Uniform Resource Identifier (URI), the ESC shall strip away any prefix digits and shall add the leading "+" character to the commercial numbers which shall be composed of the country code (CC) and national specific numbers. The SUT met this requirement with testing and the Vendor's LoC.

3. The ESC shall permit the provisioning of a Commercial Access Route on a per DoD Component Enclave-basis. Commercial Access Route provisioning data shall dictate whether a commercial call is routed to an MG that resides in the same local enclave as the call originator or to the SS. The SUT met this requirement with testing. The SUT routes to the respective environment commercial access route during normal and standalone operations.

e) The UCR 2013, Change 2, Section 2.12.2.1.5, includes the ASAC requirements in the subparagraphs below.

1. The ESC shall support the ASAC requirements for the SC related to voice and video session management as defined in this section and the AS-SIP 2013 (subject to the modifications and additions set forth in this subsection). The SUT met this requirement with testing and the Vendor’s LoC.

2. To regulate IP access link utilization, the ESC shall manage a separate voice and video budget for each of its served enclaves. The SUT met this requirement with testing.

3. The ESC shall provide the capability for the system administrator to configure a separate voice and video budget for each enclave. The SUT met this requirement with testing.

4. In the execution of centralized line-side ASAC enforcement, the ESC shall be capable of assigning calls to or from a served EI to the correct ASAC budget. In the execution of this capability, the ESC shall leverage end user/EI-to-enclave association data determined at the time of end user/EI registration as described in Section 2.12.2.1.1. The SUT met this requirement with testing and the Vendor’s LoC.

5. To enable the correct execution of ASAC, the ESC shall be able to differentiate between intra-enclave calls (which will not consume IP access link bandwidth) and inter-enclave calls (which will consume IP access link bandwidths): The ESC shall increment the corresponding ASAC budget based upon each inter-enclave session origination. The ESC shall, likewise, decrement the corresponding ASAC budgets based upon each inter-enclave session termination. The ESC shall not increment, or decrement ASAC budgets based upon intra-enclave session originations or terminations. The SUT met this requirement with testing and the Vendor’s LoC.

6. The ESC shall be capable of supporting up to 500 ASAC budgets across the ESA. The SUT met this requirement with the Vendor’s LoC.

7. With regards to the management of voice and video call counts across IP access links internal to the ESA, the ESC shall not be subject to ASAC policing by the SS. This requirement was not tested but was determined by JITC analysis to be compliant based on previous test data collected on the same hardware platform with similar performing software, product maturity, and the Vendor’s LoC.

2) The UCR 2013, Change 2, Section 2.12.2.2, includes requirements for the Centralized Enterprise Hosted UC Services requirements in the subparagraphs below.

a) The UCR 2013, Change 2, Section 2.12.2.2.1, includes the UC audio and video conferencing requirements in the subparagraphs below.

1. The centralized ESC shall provide AS-SIP based audio and video conferencing capabilities by means of a collocated UC audio and video conference system. Video from the ESC to the WAN is AS-SIP. Video internal to the ESC is not AS-SIP. The SUT met this requirement with testing with the Cisco Meeting Server (CMS).

2. The ESC shall be in the signaling path for all signaling messages exchanged between EIs served by the ESC and the associated audio and video conference system. The SUT met this requirement with testing with the CMS.

3. The conference system is not required to understand or act upon call precedence or to support the preemption of participants or conferences. The SUT met this requirement with testing with the CMS.

4. The conference system shall provide a "service portal" for end user access to UC conferencing services, features, and capabilities. The SUT met this requirement with testing with the CMS.

5. The conference system shall provide notification of participants joining and leaving a conference and provide an end-of-conference warning to all participants. The SUT met this requirement with testing with the CMS.

6. The conference system shall provide the following conferencing chair control functionality: voice-activated switching, continuous presence, mute and unmute all conference participants, enable/disable extension of a conference, and capability to "force disconnect" select participants from a conference. The SUT met this requirement with testing with the CMS.

7. A video conference system shall be capable of accepting audio-only participants into a conference call. The SUT met this requirement with testing with the CMS.

8. Audio conference systems shall support the following audio codecs: G.711, G.722. The SUT met this requirement with testing and the Vendor's LoC.

9. Audio conference systems shall optionally support the following audio codecs: G.722.1, G.723.1, G.728, G.729/G.729A. The SUT met the optional audio codecs requirements with testing and the Vendor's LoC.

10. Video conference systems shall support the following audio codecs: G.711, G.722 and G.722.1. The SUT met the audio codec requirements with testing and the Vendor's LoC.

11. Video conference systems shall optionally support the following audio codecs: G.722.1, G.723.1, G.728, G.729/G.729A and video codecs: H.261, H.263v3 (H.263 2000), and H.264 Scalable Video Coding (SVC). The SUT met the optional audio codec

requirements with testing and the Vendor's LoC. The SUT also met the optional video codec requirements with the exception of the H.264 SVC.

12. The conference system shall provide a Reservationless, Meet-Me Audio Conference service. The SUT met this requirement with testing with the CMS.

13. The conference system shall provide an Ad hoc Audio Conference service. The SUT met this requirement with testing with the CMS.

14. The conference solution shall provide a Scheduled Audio Conference service. The SUT met this requirement with testing with the CMS.

15. The conference solution shall provide Preset Conferencing capabilities. The SUT does not support Preset Conferencing. DISA accepted the Vendor's POA&M and adjudicated this discrepancy as minor.

b) The UCR 2013, Change 2, Section 2.12.2.2.2, includes the announcements and music on hold requirements in the subparagraphs below. The SUT met these requirements with testing and the Vendor's LoC.

1. The ESC shall be capable of centrally providing announcements for served EIs without a noticeable degradation in the quality of the audio transmission. The delivery of the announcement shall not be adversely impacted by traversing Enterprise or DoD Component cybersecurity accreditation boundaries (using protocols that are approved by the PPSM CAL) or by WAN transport impairments (e.g., delay, packet loss). The SUT met these requirements with testing and the Vendor's LoC.

2. The ESC shall centrally provide the set of announcements required of an SC as defined in this section. The SUT met this requirement with testing.

3. If the ESC provides music-on-hold capabilities, the music-on-hold shall be implemented as defined in AS-SIP 2013. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

c) The UCR 2013, Change 2, Section 2.12.2.2.3, includes the enterprise E911 call management requirements in the subparagraphs below.

1. The ESC shall support an integrated E911 Management capability that enables EI location information to be provided to the local emergency response dispatch center (e.g., an off-base or on-base PSAP) that is associated with each enclave within the ESA. The SUT met this requirement with the Vendor's LoC.

2. For each enclave served by the ESC, the integrated E911 Management capability shall support the generation of enclave-specific Private Switch (PS)/Automatic Location Information (ALI) database records that maps ERLs to corresponding Emergency

Location Identification Numbers (ELINs) as described in Section 3, Auxiliary Services. The SUT met this requirement with the Vendor's LoC.

3. After the individual PS/ALI database records have been generated, the integrated E911 Management solution shall be capable of exporting the enclave-specific PS/ALI record to the ALI database provider associated with the local off-base or on-base PSAP that is geographically responsible for the 911 caller. The integrated E911 Management solution shall be capable of exporting the enclave-specific PS/ALI records using the file formats defined in Section 3, Auxiliary Services. The SUT met this requirement with the Vendor's LoC.

4. The provisioning capabilities associated with the ESC's integrated 911 Management solution shall permit the manual association of an end user/EI to an ERL based upon the physical location of the end user/EI at the time of end user/EI provisioning. The SUT met this requirement with the Vendor's LoC.

5. During the end user/EI registration process, the ESC optionally shall prompt the user to establish/update their location leveraging the display capabilities of the associated softphone or hardphone. The SUT does not support this optional requirement.

6. Based on available end user/EI-to-ERL association data, the integrated E911 management capabilities shall permit the ESC to dynamically determine the correct ELIN to associate with each EI that originates a 911 emergency call. The SUT met this requirement with the Vendor's LoC.

7. If the integrated E911 management capability cannot determine the physical location of the EI originating the 911 call (i.e., it does not have specific EI-to-ERL association data for the EI that is originating the 911 call), it shall assign an enclave-specific "default ERL" to the call based on EI-to-enclave association data the ESC established during the EI registration process (see Section 2.12.2.1.1). The integrated E911 management solution shall be capable of generating and exporting ALI database records for the default ERL and the associated ELIN. The ALI record associated with the default ERL shall include: The address associated with the main Listed Directory Number (LDN) for the associated B/P/C/S location. An explicit notification that the caller's detailed location is not known and that a default routing of the emergency call has occurred. Contact information for on-site emergency personnel. The SUT met this requirement with the Vendor's LoC.

8. Using ISDN PRI trunks off an MG in the same enclave as the 911 caller, the ESC shall route the emergency call to the regional 911 network provider who is responsible for routing the emergency call to the PSAP that is geographically responsible for the 911 caller. The SUT met this requirement with the Vendor's LoC.

9. Prior to sending the call to the 911 network provider, the ESC's MGC capability shall substitute the appropriate ELIN number in place of the original Calling Party Number in the ISDN PRI setup message as described in Section 3 of the UCR. The ELIN will enable the proper routing of the call and location identification at the appropriate PSAP. The SUT met this requirement with the Vendor's LoC.

10. The ESC shall be capable of routing a "911 PSAP call back" to the EI that originated the 911 call. In the process of substituting the original Calling Party Number with an ELIN, the ESC shall temporarily cache the telephone number of the EI from which the 911 call was made (indexed against the corresponding ELIN). In the event that the PSAP dispatcher calls back using the ELIN, the ESC shall use the cached telephone number to route the "call back" to the EI that initiated the 911 call. The SUT met this requirement with the Vendor's LoC.

d) The UCR 2013, Change 2, Section 2.12.2.2.4, includes the voicemail and Unified Messaging requirements. The SUT does not support this conditional requirement.

e) The UCR 2013, Change 2, Section 2.12.2.2.5, includes the IM/Chat/Presence federation requirements in the subparagraphs below.

1. The ESC shall support secure Extensible Messaging and Presence Protocol (XMPP) server-to-server federation (i.e., server-to-server interoperability) in support of near real-time, text-based messaging (including instant messaging, group chat, and the exchange of presence) IAW the UC XMPP 2013. This requirement was met with testing and the Vendor's LoC.

2. In support of IM/Chat/Presence services within the ESA, the ESC shall provide secure client-to-server connections to served EIs. The client-to-server protocol from the ESC to the EI shall be either XMPP or vendor-proprietary (e.g., a vendor specific implementation of SIP/SIMPLE). The SUT met this requirement with the Vendor's LoC.

3. If vendor-proprietary, client-to-server protocols are used, the proprietary protocols shall be able to federate with native XMPP servers through the use of an XMPP gateway implementation that provides the bidirectional translation between XMPP and the proprietary protocol as defined in the UC XMPP 2013. The SUT does not support conditional client-to-server protocols.

f) The UCR 2013, Change 2, Section 2.12.2.2.6, includes the Enterprise Directory Services (EDS) requirements. The EDS GW requirement was not tested but was determined by JITC analysis to be compliant based on previous test data collected on the same hardware platform with similar software. The previous test data used for analysis was from the LiteScape Technologies OnCast Directory with Software Release 4.5 (APLITS tracking number 2023701) registered to the ESC 15 Software Release 12.5.1.

g) The UCR 2013, Change 2, Section 2.12.2.2.7, states the ESC shall centrally support the minimum set of requirements to capture basic call information for accounting purposes as defined in Section 2.19.2.3, Accounting Management. The SUT met this requirement with testing and the Vendor's LoC.

h) The UCR 2013, Change 2, Section 2.12.2.2.8, states the ESC shall provide a default diversion of all unanswered calls above ROUTINE precedence to a designated Directory Number (DN) (e.g., an attendant console) as defined in this section. The designated DN shall be a DN associated with an EI (e.g., an attendant console) in the same enclave as the original called party. The SUT met this requirement with testing and the Vendor's LoC to a designated DN.

3) The UCR 2013, Change 2, Section 2.12.3, includes requirements for the edge infrastructure. This section includes additional requirements for End instruments (PEI and AEI), MG, and Continuity of Operations (COOP) served by an ESC. With the exception of the AEI requirements, which are optional for the SUT, and the Preset Conferencing for COOP, the SUT met these requirements though testing and LoC. The Preset Conferencing is a documented deficiency that is discussed in Table 1 with a Plan of Action and Milestone provided by the vendor and accepted by DISA.

4) The UCR 2013, Change 2, Section 2.12.4, includes requirements for the Session Border Controller (SBC). SBCs deployed within the Enterprise UC Services architecture shall support SBC functionality defined in this section. The ESC APL SUT shall offer Enclave-Fronting SBC solutions that meet High Available SBC or Medium Available SBC requirements as defined in this section. The ESC-fronting SBC shall be a High Available SBC as defined in this section. The SUT met these requirements with testing and the Vendor's LoC.

m. The UCR 2013, Change 2, Section 2.14, includes requirements for the Call Connection Agent (CCA) function in the SC and SS. Both of these appliances have a DISN-defined design that includes Session Control and Signaling functions. These functions include both a Signaling Protocol Interworking Function (IWF) and an MGC function. The CCA described in the following requirements is part of the SCS functions and includes both the IWF and the MGC. The SUT met these requirements with testing.

1) The UCR 2013, Change 2, Section 2.14.1, includes requirements for the CCA in an SS or SC to be able to support multiple MGs on a single ASLAN, multiple ASLANs, or multiple physical locations. The SUT met these requirements with testing and the Vendor's LoC.

2) The UCR 2013, Change 2, Section 2.14.2, includes the Functional requirements of the CCA to include the IWF and MGC Component. The SUT met these requirements with testing.

3) The UCR 2013, Change 2, Section 2.14.4, includes requirements for CCA-IWF Signaling Protocol Support. This section includes the requirements for the CCA Signaling Protocol IWF to support the various VoIP and TDM signaling protocols used in the SC and SS. The role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that are used by the EIs, MGs, and SBCs, and interwork all these various signaling protocols with one another. The SUT met these requirements with testing and the Vendor's LoC.

a) The UCR 2013, Change 2, Section 2.14.4.1, includes the requirements for CCA-IWF support for AS-SIP. The SUT met these requirements with testing and the Vendor's LoC.

b) The UCR 2013, Change 2, Section 2.14.4.2, includes the requirements for CCA-IWF Support for PRI via MG. The SUT met these requirements with testing and the Vendor's LoC.

c) The UCR 2013, Change 2, Section 2.14.4.3, includes the optional requirements for CCA-IWF Support for CAS Trunks via MG. The SUT supports CAS interfaces but they were not tested and are not included in this certification.

d) The UCR 2013, Change 2, Section 2.14.4.4, includes the requirements for CCA-IWF Support for PEI and AEI Signaling Protocols. The SUT AEI signaling protocol was not tested because there were no AEIs submitted with the SUT. In addition, there are no AEIs on the DoDIN APL certified with the SUT. The SUT met the requirements with testing with the voice and video PEI interfaces only.

e) The UCR 2013, Change 2, Section 2.14.4.5, includes the requirements for CCA-IWF Support for VoIP and TDM Protocol Interworking. The SUT met these requirements with the SUT MGs that internetwork VoIP with analog and digital T1/E1 TDM interfaces.

n. The UCR 2013, Change 2, Section 2.15, includes the requirements for CCA Interaction with Network Appliances and Functions.

1) The UCR 2013, Change 2, Section 2.15.1, includes the requirements for CCA interaction with transport interface functions. The Transport Interface functions in an appliance provide interface and connectivity functions with the ASLAN and its IP packet transport network. The SUT met these requirements with testing and the Vendor's LoC.

2) The UCR 2013, Change 2, Section 2.15.2, includes the requirements for CCA interactions with the SBC requirements. The SUT met these requirements with testing and the Vendor's LoC.

3) The UCR 2013, Change 2, Section 2.15.3, includes the requirements for CCA support for Admission Control requirements. The CCA interacts with the ASAC component of the SC and SS to perform specific functions related to ASAC, such as counting internal, outgoing, and incoming calls; managing separate call budgets for VoIP and Video over IP calls; and providing preemption. The SUT met these requirements with testing and the Vendor's LoC.

4) The UCR 2013, Change 2, Section 2.15.4, includes the requirements for CCA support for User Features and Services. The User Features and Services (UFS) Server is responsible for providing features and services to VoIP and Video PEIs/AEIs on an SC or SS, where the CCA alone cannot provide the feature or service. This requirement states that the CCA within a network appliance shall support the operation of the following features and capabilities: The CCA shall generate a redirecting number each time it forwards a VoIP or Video session request as part of a CF feature. The CCA supports the ability to direct VoIP and Video sessions and session requests to the UFS Server, so that the UFS Server can apply an Appliance VoIP or Video feature, when use of that feature is required by the calling party, the called party, or the appliance itself. The SUT met these requirements with testing with the voice and video PEI interfaces only.

5) The UCR 2013, Change 2, Section 2.15.5, includes the requirements for CCA Support for CS. The CS function within the appliance ensures that end users, PEIs, AEIs, MGs, and SBCs that use the appliance are all properly authenticated and authorized by the appliance. The CS function ensures that voice and video signaling streams that traverse the appliance and its ASLAN are properly encrypted SIP/Transport Layer Security (TLS). The SUT met these requirements with testing and the Vendor's LoC and is certified with voice and video PEI interfaces only. The SUT encrypts media with Secure Real-time Transport Protocol (SRTP) and signaling with TLS. In addition, the JITC-led CS test team conducted security testing and published the results in a separate report, Reference (d).

6) The UCR 2013, Change 2, Section 2.15.8, includes the requirements for CCA interactions with EIs. The CCA in the SS or SC needs to interact with VoIP PEIs and AEIs served by that SS or SC. The VoIP interface between the PEI and the SS or SC is left up to the network appliance supplier. The VoIP interface between the AEI and the SS or SC is AS-SIP. The SUT met these requirements with testing with the voice and video PEIs.

7) The UCR 2013, Change 2, Section 2.15.9, includes the requirements for CCA support for Assured Services voice and video. The Appliance CCA shall support both assured voice and video services. The CCA shall support both assured voice and assured video sessions, and shall support these sessions from both, VoIP EIs and Video EIs, as described in Section 2.15.8, CCA Interactions with End Instrument(s). The SUT met these requirements with testing and the Vendor's LoC.

8) The UCR 2013, Change 2, Section 2.15.10, includes the requirements for CCA interactions with service control functions. The CCA shall support the ability to remove VoIP and video sessions and session requests from the media server so the CCA can continue with necessary session processing once the media server has completed its functions. The SUT met these requirements with the Vendor's LoC.

o. The UCR 2013, Change 2, Section 2.16, includes requirements for the MG function in the SC and SS network appliances. These appliances have defined designs that include an MGC function and one or more MGs.

1) The UCR 2013, Change 2, section 2.16.1, includes the requirements for MG call denial treatments to support CAC requirements. When the CCA determines that a VoIP session request should be blocked because an Appliance CAC restriction applies, the CCA will deny the session request and apply a Call Denial treatment to the calling party on that request. The SUT met this requirement with the Vendor's LoC.

a) The UCR 2013, Change 2, Section 2.16.1.1, includes the requirements for MG call preemption treatments to Support ASAC. The SUT met these requirements with testing and the Vendor's LoC.

b) The UCR 2013, Change 2, Section 2.16.1.2, includes the requirements for MG and Information Assurance functions. The JITC-led CS test team completed security testing and published the results in a separate report, Reference (d).

c) The UCR 2013, Change 2, section 2.16.1.3, states that the media server is responsible for playing tones and announcements to calling and called parties on VoIP calls, and for playing audio/video clips (similar to tones and announcements) to calling and called parties on video calls. The MG is responsible for routing individual VoIP, Facsimile (Fax) over IP (FoIP), and Modem [Relay] over IP (MoIP) media streams to the media server when instructed to do so by the CCA/MGC. When instructed to do so by the MGC, the MG shall direct TDM calls and call requests to the media server, so that the media server can do the following: Play tones and announcements to TDM parties on TDM calls and call requests (e.g., busy tone or announcement; call preemption tone or announcement). Provide "play announcement and collect digits" functionality when required by an Appliance VoIP feature. Provide full Interactive Voice Response (IVR)-like functionality when required by an Appliance VoIP feature. The SUT met these requirements with testing and the Vendor's LoC.

d) The UCR 2013, Change 2, Section 2.16.1.4, includes the requirements for interactions with IP Transport interface functions. The SUT met these requirements with testing and the Vendor's LoC.

e) The UCR 2013, Change 2, Section 2.16.1.5, includes the requirements for MG–SBC interaction. The SUT met these requirements with testing and the Vendor's LoC.

f) The UCR 2013, Change 2, Section 2.16.1.6, states the Management function in the SBC, SC, and SS supports functions for SBC/SC/SS FCAPS management and audit logs. The MG shall interact with the Appliance Management function by doing the following: Making changes to its configuration and to its trunks' configuration in response to commands from the Management function that request these changes. Returning information to the Management function on its FCAPS in response to commands from the Management function that request this information. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on MG activity. The SUT met these requirements with the Vendor's LoC.

g) The UCR 2013, Change 2, Section 2.16.1.8, states the MG shall support the exchange of VoIP media streams with the following voice PEIs and AEIs both on the local appliance and on remote network appliances: Vendor proprietary Voice PEIs; Voice SIP EIs, when the appliance supplier supports these EIs; Voice H.323 EIs, when the appliance supplier supports these EIs; Voice AS-SIP EIs. The SUT does not support this optional requirement.

h) The UCR 2013, Change 2, Section 2.16.1.9, states the MG shall support the operation of the following features for VoIP and Video end users, consistent with the operation of this feature on analog and ISDN lines in DoD TDM switches: Call Hold, Music on Hold, Call Waiting, Precedence Call Waiting, Call Forwarding Variable, Call Forwarding Busy Line, Call Forwarding No Answer, Call Transfer, Three-way calling, Hotline Service, Calling Number Delivery, and Call Pickup. The SUT met this requirement with testing and the Vendor's LoC.

i) The UCR 2013, Change 2, Section 2.16.2, includes requirements for MG interfaces to TDM NEs in DoD networks. Each appliance MG shall support TDM trunk groups that can interconnect with the following NEs in DoD networks, in the United States (U.S.) and worldwide: Private Branch Exchanges, Small End Offices, End Offices), and Multifunction Switches. Each appliance MG shall support TDM trunk groups that can interconnect with DISN and DoD NEs in the United States and worldwide using ISDN PRI ANSI T1.619a. The appliance MG may optionally support CAS. The SUT met these requirements with testing and the Vendor's LoC with the following exception: The SUT allows an external equal or lower precedence above Routine caller via ISDN T1 PRI (ANSI T1.619a) to preempt an equal or higher above Routine SUT IP subscriber. DISA accepted the Vendor's POA&M and adjudicated this exception as minor with the following condition of fielding: The SUT IP EIs will be configured with two call-appearances, and precedence outbound dialing by the IP user can be accomplished with soft-keys in lieu of dialing 9 plus precedence (i.e., 93, 92, etc.). The SUT supports CAS interfaces but they were not tested and are not included in this certification.

2) The UCR 2013, Change 2, Section 2.16.3, includes requirements for MG interfaces to TDM NEs in Allied and Coalition Partner Networks. The appliance suppliers should support TDM trunk groups on their MG product that can interconnect with NEs in U.S. Allied and Coalition partner networks worldwide. The MG shall support foreign country ISDN PRI trunk groups where the MG handles both the media channels and the signaling channel as follows: For interconnection with an allied or coalition partner network, using foreign ISDN PRI from the network of the allied or coalition partner. Support for MLPP using ISDN PRI, per ITU-T Recommendation Q.955.3 (ISDN Signaling Standard for E1 MLPP), is required on SC trunk groups when these trunk groups are used to connect to an allied or coalition partner from a U.S. Outside the Continental U.S. (OCONUS) European Telecommunications Standards Institute (ETSI)-compliant country. The SUT met this requirement with testing and the Vendor's LoC with the following exception: The SUT allows an external equal or lower precedence above Routine caller via ISDN T1 PRI (ANSI T1.619a) to preempt an equal or higher above Routine SUT IP subscriber. DISA accepted the Vendor's POA&M and adjudicated this exception as minor with the following condition of fielding: The SUT IP EIs will be configured with two call-appearances, and precedence outbound dialing by the IP user can be accomplished with soft-keys in lieu of dialing 9 plus precedence (i.e., 93, 92, etc.).

3) The UCR 2013, Change 2, Section 2.16.4, includes MG Interfaces to TDM NEs in the PSTN in the U.S. Each appliance MG shall support TDM trunk groups that can interconnect with NEs in the PSTN in the United States, including Continental U.S. (CONUS), Alaska, Hawaii, and U.S. Caribbean and Pacific Territories. Each appliance MG shall support TDM trunk groups that can interconnect with the U.S. PSTN, using the following types of trunk groups: U.S. National ISDN PRI, where the MG handles both the media channels and the signaling channel is required for U.S. PSTN nationwide; support for Facility Associated Signaling is required; support for MLPP is not required; support for Non-Facility Associated Signaling is optional. CAS is optional for U.S. PSTN NEs nationwide. The SUT met these requirements with testing and the Vendor's LoC.

4) The UCR 2013, Change 2, Section 2.16.5, includes requirements for MG interfaces to TDM NEs in OCONUS PSTN Networks. The appliance supplier (i.e., SC or SS supplier) should support TDM trunk groups on its MG product that can interconnect with NEs in foreign country PSTN networks (OCONUS) worldwide. The MG shall support foreign country ISDN PRI, where the MG handles both the media channels and the signaling channel: For interconnection

with a foreign country PSTN, using foreign country ISDN PRI, from the country where the DoD user's B/P/C/S is located. Support for ETSI PRI is required on SC trunk groups when the SC is used in OCONUS ETSI-compliant countries. Support for MLPP using ISDN PRI is not required on these trunk groups. The SUT met these requirements with testing and the Vendor's LoC.

5) The UCR 2013, Change 2, Section 2.16.6, includes the requirements for MG support for ISDN PRI trunks. The SUT met these requirements with testing and the Vendor's LoC.

6) The UCR 2013, Change 2, Section 2.16.7, includes the optional requirements for MG support for CAS trunks. The SUT supports CAS interfaces but they were not tested and are not included in this certification.

7) The UCR 2013, Change 2, Section 2.16.8, includes the requirements for MG requirements: VoIP Interfaces Internal to an Appliance. The requirements in this section assume that a supplier-specific Gateway Control Protocol is used on the MGC-MG interface. The SUT met these requirements with the Vendor's LoC.

8) The UCR 2013, Change 2, Section 2.16.9, includes the requirements for Echo Cancellation. The requirements in this section are based on the commercial VoIP network Echo Cancellation requirements in Telcordia Technologies GR-3055-CORE. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

9) The UCR 2013, Change 2, Section 2.16.10, includes the requirements for MG requirements for clock timing. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

10) The UCR 2013, Change 2, Section 2.16.11, includes the requirements for MGC-MC CCA Functions. The MGC within the CCA shall be responsible for controlling all the MGs within the SC or SS. The MGC within the CCA shall be responsible for controlling all the trunks (i.e., PRI or CAS) within each MG within the SC or SS. The MGC within the CCA shall be responsible for controlling all media streams on each trunk within each MG. The SUT met these requirements with PRI with testing and the Vendor's LoC. The SUT supports CAS interfaces but they were not tested and are not included in this certification.

11) The UCR 2013, Change 2, Section 2.16.12, states that the MG uses ITU-T Recommendation V.150.1, then the following applies: ITU-T Recommendation V.150.1 provides for three states: audio, VBD, and modem relay. After call setup, inband signaling may be used to transition from one state to another. In addition, V.150.1 provides for the transition to FoIP using Fax Relay per ITU-T Recommendation T.38. When the MG uses V.150.1 inband signaling to transition between audio, FoIP, modem relay, or VBD states or modes, the MG shall continue to use the established session's protocol (e.g., decimal 17 for User Datagram Protocol) and port numbers so that the transition is transparent to the SBC. The SUT met these requirements with testing and the Vendor's LoC.

12) The UCR 2013, Change 2, Section 2.16.13, includes the conditional requirements for Remote Media Gateway. If the MG is geographically separated from the MGC that controls it, then the five specific conditional requirements in this section that address the SBC, the MG control protocol, the DSCP for the control packets, and the security aspects for that arrangement apply. The SUT met these conditional requirements with the Vendor's LoC.

p. The UCR 2013, Change 2, Section 2.18, includes the requirements for the Worldwide Numbering and Dialing Plan (WWNDP).

1) The UCR 2013, Change 2, Section 2.18.1, includes the requirements for DSN WWNDP. The SUT met these requirements with testing and the Vendor's LoC.

2) The UCR 2013, Change 2, Section 2.18.1.1, includes the requirements for CCA and Softswitch Location Service support for dual assignment of DSN and E.164 numbers to SS EIs. The SUT met these requirements with testing and the Vendor's LoC.

3) The UCR 2013, Change 2, Section 2.18.1.2, includes the requirements for CCA differentiation between DSN numbers and E.164 numbers. The SUT met these requirements with testing and the Vendor's LoC.

4) The UCR 2013, Change 2, Section 2.18.1.3, includes the optional requirements for CCA use of SIP "phone-context" to differentiate between DSN and E.164 numbers. The SUT does not support this optional requirement.

5) The UCR 2013, Change 2, Section 2.18.1.4, includes the optional requirements for use of SIP URI domain name with DSN numbers and E.164 numbers. The SUT met these requirements with the Vendor's LoC.

6) The UCR 2013, Change 2, Section 2.18.1.5, includes the requirements for Domain Directory. The SUT met these requirements with testing and the Vendor's LoC.

q. The UCR 2013, Change 2, Section 2.19, includes the requirements for the management of network appliances.

1) The UCR 2013, Change 2, Section 2.19.1, includes the general management requirements for the management of network appliances. The SUT met these requirements with the Vendor's LoC.

2) The UCR 2013, Change 2, Section 2.19.2, includes the requirements for FCAPS Management. General requirements for the five management functional areas are defined in the subparagraphs below.

a) The UCR 2013, Change 2, Section 2.19.2.1, includes the requirements for Fault Management. The SUT met these requirements with the Vendor's LoC.

b) The UCR 2013, Change 2, Section 2.19.2.2, includes the requirements for Configuration Management. The SUT met these requirements with the Vendor's LoC.

c) The UCR 2013, Change 2, Section 2.19.2.3, includes the requirements for Accounting Management. The SUT met these requirements with the Vendor's LoC.

d) The UCR 2013, Change 2, Section 2.19.2.4, includes the requirements for Performance Management. The SUT met these requirements with the Vendor's LoC.

e) The UCR 2013, Change 2, Section 2.19.2.5, states that all network management interactions shall meet the access control, confidentiality, integrity, availability, and non-repudiation requirements in Section 4, Cybersecurity. The JITC-led CS test team completed security testing and published the results in a separate report, Reference (d).

r. The UCR 2013, Change 2, Section 2.20, includes the conditional requirements for V.150.1 modem relay secure phone support. The SUT met these requirements with testing and the Vendor's LoC.

s. The UCR 2013, Change 2, Section 2.21, includes the conditional requirements for supporting AS-SIP-based Ethernet interfaces for voicemail systems. The SUT does not support this conditional requirement.

t. The UCR 2013, Change 2, Section 2.22, includes the optional requirements for Local Attendant Console Features. The SUT does not support this optional requirement.

u. The UCR 2013, Change 2, Section 2.23, includes the optional requirements for Master Session Controllers (MSCs) and Subtended Session Controllers (SSCs). This requirement applies to the SUT in the LSC configuration. This optional configuration was not tested and is not included in this certification.

v. The UCR 2013, Change 2, Section 2.24, includes the optional requirements for MSC, SSC, and dynamic ASAC requirements in support of bandwidth-constrained links. This requirement applies to the SUT in the LSC configuration. This optional configuration was not tested and is not included in this certification.

w. The UCR 2013, Change 2, Section 2.25, includes the requirements for MLPP.

1) The UCR 2013, Change 2, Section 2.25.1, includes the requirements for MLPP. In general, the MLPP requirements in this section apply to IP-based Precedence-Based Assured Services (PBAS), i.e., the use of the term "MLPP" in this section is not meant to restrict these requirements to services provided by TDM-based networks. The MLPP service applies to the MLPP service domain only. Connections and resources that belong to a call from an MLPP subscriber shall be marked with a precedence level and domain identifier (consistent with ANSI Standards T1.619-1992 and T1.619a-1994) and shall be preempted only by calls of higher precedence from MLPP users in the same MLPP service domain.

a) The UCR 2013, Change 2, Section 2.25.1.1, states that the SC, SS, PEI and AEI shall provide five precedence levels. The precedence levels listed from lowest to highest are ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE. The SUT met this requirement with testing and the Vendor's LoC.

b) The UCR 2013, Change 2, Section 2.25.1.2, includes the requirements for invocation and operation. The SUT met these requirements with testing.

c) The UCR 2013, Change 2, Section 2.25.1.3, includes the requirements for preemption in the network. The SUT met these requirements with testing with the following exception: The SUT allows an external equal or lower precedence above Routine caller via ISDN T1 PRI (ANSI T1.619a) to preempt an equal or higher above Routine SUT IP subscriber denoted in the memorandum Conditions Table 1. DISA accepted the Vendor's POA&M and adjudicated this discrepancy as minor with the following condition of fielding: The SUT IP EIs will be configured with two call-appearances, and precedence outbound dialing by the IP user can be accomplished with soft-keys in lieu of dialing 9 plus precedence (i.e., 93, 92, etc.).

d) The UCR 2013, Change 2, Section 2.25.1.4, includes the requirements for preempt signaling. The SUT met these requirements with testing and the Vendor's LoC.

e) The UCR 2013, Change 2, Section 2.25.1.5, includes the requirements for analog line MLPP. The SUT met these requirements with testing and the Vendor's LoC.

f) The UCR 2013, Change 2, Section 2.25.1.6, includes the requirements for ISDN MLPP BRI. The SUT does not support this optional requirement.

g) The UCR 2013, Change 2, Section 2.25.1.7, includes the requirements for ISDN MLPP PRI. The SUT met these requirements with testing and the Vendor's LoC.

h) The UCR 2013, Change 2, Section 2.25.1.8, includes the requirements for MLPP interactions with common optional features and services. The SUT does not support this optional requirement.

i) The UCR 2013, Change 2, Section 2.25.1.9, includes the optional requirements for MLPP interactions with Electronic Key Telephone Systems (EKTS) features. The SUT does not support this optional requirement.

2) The UCR 2013, Change 2, Section 2.25.2, includes requirements for Signaling.

a) The UCR 2013, Change 2, Section 2.25.2.2, states the UC signaling appliance systems shall meet the network power systems requirements specified in the Telcordia Technologies GR-506-CORE, Paragraph 2.1. The SUT met these requirements with testing and Vendor LoC.

b) The UCR 2013, Change 2, Section 2.25.2.3, includes the requirements for line signaling. The SUT met these requirements with testing and the Vendor's LoC.

c) The UCR 2013, Change 2, Section 2.25.2.4, includes the optional requirements for trunk supervisory signaling. The SUT met these requirements with the Vendor's LoC.

d) The UCR 2013, Change 2, Section 2.25.2.5, includes the requirements for control signaling. The SUT met these requirements with testing and the Vendor's LoC.

e) The UCR 2013, Change 2, Section 2.25.2.7, includes the requirements for ISDN Digital Subscriber Signaling System No. 1 (DSS1) signaling. The SUT met these requirements with testing and the Vendor's LoC.

3) The UCR 2013, Change 2, Section 2.25.3, includes requirements for ISDN. The UC signaling appliance systems shall provide the ISDN BRI and PRI capabilities shown in Tables 2.25-9 through 2.25-13 as annotated in the tables. The requirements for PRI access, call control, and signaling in Table 2.25-12 are required. The SUT met these requirements with testing and the Vendor's LoC for ISDN PRI. The SUT does not support the optional ISDN BRI.

4) The UCR 2013, Change 2, Section 2.25.4, includes requirements for backup power. UC shall have backup power to maintain continuous operation whenever the primary source of power is disrupted. Back-up power design and implementation shall be incorporated into the design. General power requirements are described in Telcordia Technologies GR-513-CORE. Following the risk avoidance guidance in Telcordia Technologies GR-513-CORE, the backup power design shall minimize the probability of a complete loss of UC appliance system power. This is a non-testable requirement. The SUT must be installed following this guidance.

5) The UCR 2013, Change 2, Section 2.25.5, includes Echo Canceller requirements. This section provides the requirements for echo control equipment in the UC network. All MG Echo Canceller (EC) devices are required to meet the requirements. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software, and product maturity.

a) The UCR 2013, Change 2, Section 2.25.5.1, includes the requirements for EC functionality. The SUT met these requirements with the Vendor's LoC.

b) The UCR 2013, Change 2, Section 2.25.5.2, includes the requirements for 2100-Hertz EC disabling tone capability. The SUT met these requirements with the Vendor's LoC.

c) The UCR 2013, Change 2, Section 2.25.5.3, states that the EC shall be able to be connected to either analog and/or digital transmission facilities. An analog trunk interface shall be able to provide echo cancellation on a per-trunk basis. A digital trunk interface shall be implemented on a digital basis without conversion to analog. The digital EC shall treat all Digital Signal Level 0 (DS0) channels (Pulse Code Modulation (PCM)-24, PCM-30, or more for Synchronous Optical Network (SONET)) independently. This requirement was not tested but was determined by JITC analysis to be compliant based on the Vendor's LoC and previous test data collected on the same hardware platform with similar performing software.

d) The UCR 2013, Change 2, Section 2.25.5.4, includes the requirements for Echo Cancellation on PCM circuits. The SUT met these requirements with the Vendor's LoC.

e) The UCR 2013, Change 2, Section 2.25.5.5, includes the requirements for device management. This requirement was not tested but was determined by JITC analysis to be compliant based on previous test data collected on the same hardware platform with similar performing software.

f) The UCR 2013, Change 2, Section 2.25.5.6, states that the EC reliability and availability shall conform to Section 5 of Telcordia Technologies GR-512-CORE, as specified for individual devices. The vendor shall provide a reliability model for the system, showing all calculations along with how the overall availability will be met, if requested. The SUT met this requirement with the Vendor's LoC.

6) The UCR 2013, Change 2, Section 2.25.6, includes the requirements for VoIP system latency for MG trunk traffic. This requirement was not tested but was determined by JITC analysis to be compliant based on previous test data collected on the same hardware platform with similar performing software.

x. The UCR 2013, Change 2, Section 4, includes the CS requirements. These requirements are based on DISA Facility Security Office (FSO) STIGs and Security Requirement Guides (SRGs). The STIGs and SRGs now serve as a primary baseline for purely CS-focused requirements, and this UCR section focuses on those requirements that impact interoperability from a CS standpoint. The JITC-led CS test team completed security testing and published the results in a separate report, Reference (d).

y. The UCR 2013, Change 2, Section 5, includes the IPv6 requirements. The SC/CCA application in conjunction with the VVoIP EI and MG must be IPv6-capable. The guidance in Table 5.2-4 for Network Appliance/Simple Server (NA/SS) applies. In addition, the requirements throughout section 5 for NA/SS apply. The SUT met these requirements with testing and the Vendor's LoC.

z. AS-SIP 2013 is the standard signaling protocol used within the DoD information systems networks that provide end-to-end Assured Services. This section defines requirements for AS-SIP signaling requirements for operation within an IP-only network infrastructure and for inter-working between IP network segments and legacy TDM network segments in a hybrid IP and TDM network infrastructure. The SUT met these requirements with testing.

7. HARDWARE/SOFTWARE/FIRMWARE VERSION IDENTIFICATION. Table 3-3 provides the SUT components' hardware, software, and firmware tested. The SUT was tested 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.

8. TESTING LIMITATIONS. Due to limitations in the test architecture, end-to-end IPv6 testing was not conducted. JITC conducted intra-enclave IPv6 testing only. The SUT met the IPv6 requirements with testing and the Vendor's LoC.

9. CONCLUSION(S). The SUT meets the critical interoperability requirements as an ESC in Type 1, 2, and 3 environments and as an LSC IAW the UCR, Reference (b), and is certified for joint use with other DoDIN products listed on the APL with the conditions described in Table 1.

DATA TABLES

Table 3-1. SUT Interface Status

Interface (See note 1.)	Applicability	Status	Remarks
Network Management Interfaces			
10BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3i interface.
100BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3u interface.
1000BaseT	C	Met	The SUT met the critical CRs and FRs for the IEEE 802.3ab interface.
Network Interfaces (Line and Trunk)			
10BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3i interface with the SUT PEIs and softphones.
100BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3u interface with the SUT PEIs and softphones.
1000BaseT	R	Met	The SUT met the critical CRs and FRs for the IEEE 802.3ab interface with the SUT video PEIs and softphones
2-wire analog	R	Met	The SUT met the critical CRs and FRs for the 2-wire analog interface with the SUT 2-wire secure and non-secure analog instruments.
ISDN BRI	C	Not Tested	The SUT does not support this conditional interface.
Legacy Interfaces (External)			
ISDN T1 PRI (ANSI T1.619a)	R	Partially Met (See note 2.)	The SUT partially met the critical CRs/FRs. This interface provides legacy DSN and TELEPORT connectivity.
ISDN T1 PRI NI-2	R	Met	The SUT met the critical CRs/FRs. This interface provides PSTN connectivity.
T1 CCS7 (ANSI T1.619a)	C	Not Tested	The SUT does not support this conditional interface.
T1 CAS	C	Not Tested	The SUT supports this interface, but it was not tested and not included in this certification.
E1 PRI (ITU-T Q.955.3)	C	Partially Met (See note 2.)	The SUT partially met the critical CRs/FRs. This interface provides OCONUS MLPP connectivity in ETSI-compliant countries.
E1 PRI (ITU-T Q.931)	C	Met	The SUT met the critical CRs/FRs. This interface provides PSTN connectivity in ETSI-compliant countries.
E1 CAS	C	Not Tested	The SUT supports this interface, but it was not tested and not included in this certification.

NOTE(S):
1. Table 3 depicts the SUT high-level requirements. Refer to Enclosure 3, Table 3-2, for a detailed list of requirements.
2. The SUT met the requirements with the exceptions noted in Table 1. DISA accepted the Vendor's POA&M and adjudicated these exceptions as minor.

LEGEND:

ANSI	American National Standards Institute
BaseT	Megabit Ethernet
BRI	Basic Rate Interface
C	Conditional
CAS	Channel Associated Signaling
CCS7	Common Channel Signaling Number 7
CR	Capability Requirement
DISA	Defense Information Systems Agency
DSN	Defense Switched Network
E1	European Basic Multiplex Rate (2.048 Mbps)
ETSI	European Telecommunications Standards Institute
FR	Functional Requirement
IEEE	Institute of Electrical and Electronics Engineers
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
Mbps	Megabits per second
MLPP	Multi-Level Precedence and Preemption
NI-2	National ISDN Standard 2
OCONUS	Outside the Continental United States
PEI	Proprietary End Instrument
POA&M	Plan of Action and Milestones
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
Q.931	Signaling Standard for ISDN
Q.955.3	ISDN Signaling Standard for E1 MLPP
R	Required
SS7	Signaling System 7
SUT	System Under Test
T1	Digital Transmission Link Level 1 (1.544 Mbps)
T1.619a	SS7 and ISDN MLPP Signaling Standard for T1

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

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status
1	**Voice Features and Capabilities**			
	Voice Features and Capabilities	Required	2.2	Met
	Call Forwarding	Required	2.2.1	Met
	MLPP Interactions with Call Forwarding	Required	2.2.2	Met
	Precedence Call Waiting	Required	2.2.3	Met
	Call Transfer	Required	2.2.4	Met
	Call Hold	Required	2.2.5	Met
	Three-Way Calling	Required	2.2.6	Met
	Hotline Service	Optional	2.2.7	Met
	Calling Number Delivery	Required	2.2.8	Met
	Call Pick-Up	Optional	2.2.9	Met
	Precedence Call Diversion	Required	2.2.10	Met
	Public Safety Voice Features	Required	2.2.11	Met
2	**Assured Services Admission Control**			
	ASAC Requirements Related to Voice	Required	2.3.1	Met
	ASAC Requirements for the SC and SS Related to Video Services	Required	2.3.3	Met
3	**Signaling Protocols**			
	Signaling Performance Guidelines	Required	2.4.1	Met
4	**Registration and Authentication**			
	Registration and Authentication	Required	2.5	Met (See note 2.)
5	**SC and SS Failover and Recovery**			
	SC Failover: Alternative A: The SC-Generated OPTIONS Method	Conditional	2.6.1	Not Tested (See note 3.)
	SC Failover: Alternative B: The SBC-Generated OPTIONS Method	Conditional	2.6.2	Met
6	**Product Interface** (See note 4.)			
	Internal Interface	Required	2.7.1	Met
	External Physical Interfaces Between Network Components	Required	2.7.2	Met
	Interfaces to Other Networks	Required	2.7.3	Met
	DISA VVoIP EMS Interface	Required	2.7.4	Met
7	**Product Physical, Quality, and Environmental Factors**			
	Product Quality Factors	Required	2.8.2	Met
	Voice Service Quality	Required	2.8.4	Met
8	**End Instruments (including tones and announcements)**			
	IP Voice End Instruments	Required	2.9.1	Met
	Analog and ISDN BRI Telephone Support	Required	2.9.2	Met (See note 5.)
	Video End Instrument	Required	2.9.3	Not Tested (See note 6.)
	Authentication to SC	Required	2.9.4	Met
	EI interface to the ASLAN	Required	2.9.5	Met
	Operational Framework for AEIs and Video EIs	Required	2.9.6	Met
	Multiple Call Appearance Requirements for AS-SIP EIs	Required	2.9.7	Met
	PEIs, AEIs, TAs, and IADs Using the V.150.1 Protocol	Required	2.9.8	Met
	UC Products with Non-Assured Service Features	Conditional	2.9.9	Met
	ROUTINE-only EIs	Conditional	2.9.10	Not Tested (See note 3.)

(Table continues next page.)

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

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status
9	**Session Controller**			
	PBAS/ASAC	Required	2.10.1	Met
	SC Signaling	Required	2.10.2	Met
	Session Controller Location Service	Required	2.10.3	Met
	SC Management Function	Required	2.10.4	Met
	SC-to-VVoIP EMS Interface	Required	2.10.5	Met
	SC Transport Interface Functions	Required	2.10.6	Met
	Custom Line-Side Features Interference	Conditional	2.10.7	Not Tested (See note 3.)
	Loop Avoidance for SCs	Required	2.10.8	Met
	Local Session Controller Application	Required	2.10.9	Met
10	**AS-SIP Gateways** (See note 7.)			
	AS-SIP TDM Gateway	Conditional	2.11.1	Not Tested
	AS-SIP IP Gateway	Conditional	2.11.2	Not Tested
	AS-SIP – H.323 Gateway	Conditional	2.11.3	Not Tested
11	**Enterprise UC Services**			
	Enterprise Session Controller (ESC) Core Infrastructure	Required	2.12.2	Partially Met (See note 8.)
	Edge Infrastructure	Required	2.12.3	Met
	Session Border Controller (SBC)	Required	2.12.4	Met
12	**Call Connection Agent**			
	Introduction	Required	2.14.1	Met
	Functional	Required	2.14.2	Met
	CCA-IWF Signaling Protocol Support	Required	2.14.4	Met
13	**CCA Interaction with Network Appliances and Functions**			
	CCA Interactions with Transport Interface Functions	Required	2.15.1	Met
	CCA Interactions with the SBC	Required	2.15.2	Met
	CCA Support for Admission Control	Required	2.15.3	Met
	CCA Support for User Features and Services	Required	2.15.4	Met
	CCA Support for Information Assurance	Required	2.15.5	Met
	CCA Interactions with End Instruments	Required	2.15.8	Met
	CCA Support for Assured Services Voice and Video	Required	2.15.9	Met
	CCA Interactions with Service Control Functions	Required	2.15.10	Met
14	**Media Gateway**			
	MG Call Denial Treatments to Support CAC	Required	2.16.1	Met
	MG Interfaces to TDM NEs in DoD Networks: PBXs, EOs, and MFSs	Required	2.16.2	Partially Met (See note 8.)
	MG Interfaces to TDM NEs in Allied and Coalition Partner Networks	Required	2.16.3	Partially Met (See note 8.)
	MG Interfaces to TDM NEs in the PSTN in the United States	Required	2.16.4	Met
	MG Interfaces to TDM NEs in OCONUS PSTN Networks	Required	2.16.5	Met
	MG Support for ISDN PRI Trunks	Required	2.16.6	Met
	MG Support for CAS Trunks	Optional	2.16.7	Not Tested (See note 9.)
	MG Requirements: VoIP Interfaces Internal to an Appliance	Required	2.16.8	Met
	MG Requirements for Echo Cancellation	Required	2.16.9	Met
	MG Requirements for Clock Timing	Required	2.16.10	Met
	MGC-MG CCA Functions	Required	2.16.11	Met
	MGs Using the V.150.1 Protocol	Conditional	2.16.12	Met
	Remote Media Gateway	Conditional	2.16.13	Met

(Table continues next page.)

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

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status
15	**Worldwide Numbering & Dialing Plan**			
	Worldwide Numbering and Dialing Plan	Required	2.18.1	Met
16	**Management of Network Devices**			
	General Management	Required	2.19.1	Met
	Requirements for FCAPS Management	Required	2.19.2	Met
17	**V.150.1 Modem Relay Secure Phone Support**			
	V.150.1 Modem Relay Secure Phone Support	Required	2.20	Met
18	**Requirements for Supporting AS-SIP Based Ethernet Devices for Voicemail Systems**			
	Requirements for Supporting AS-SIP Message Waiting Indications on AS-SIP EIs, TAs, and IADs	Conditional	2.21.1	Not Tested (See note 3.)
19	**Local Attendant Console Features**			
	Local Attendant Console Features	Optional	2.22	Not Tested (See note 3.)
20	**MSC and SSC**			
	MSC and SSC	Optional	2.23	Not Tested (See note 10.)
21	**MSC, SSC, and Dynamic ASAC Requirements in Support of Bandwidth-constrained Links**			
	MSC and SSC Architecture	Optional	2.24.1	Not Tested (See note 10.)
	Dynamic ASAC	Optional	2.24.2	Not Tested (See note 10.)
22	**Other UC Voice**			
	Multilevel Precedence and Preemption	Required	2.25.1	Partially Met (See note 8.)
	Signaling	Required	2.25.2	Met
	ISDN	Required	2.25.3	Met
	Backup Power	Required	2.25.4	Not Tested (See note 11.)
	Echo Canceller	Required	2.25.5	Met
	VoIP System Latency for MG Trunk Traffic	Required	2.25.6	Met
23	**Cybersecurity Requirements**			
	Security Requirements	Required	4.2	Met (See note 2.)
24	**IPv6 Requirements**			
	IPv6	Required	5.2	Met
25	**Assured Services - Session Initiation Protocol (AS-SIP 2013)**			
	AS-SIP	Required	AS-SIP	Met

NOTE(S):
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Reference (c).
2. The JITC-led Cybersecurity test team completed security testing and published the results in a separate report, Reference (d).
3. The SUT does not support this optional/conditional requirement.
4. Refer to interface Table 3-1 for certified internal, external, and management interfaces.
5. The SUT met the requirements for analog. The SUT does not support the ISDN BRI optional interface.
6. The SUT offers H.323 Video EIs but they were not tested and are not included in this certification.
7. The SUT was not tested or certified for any of the three optional AS-SIP gateway requirements listed in UCR 2013, Change 2, Section 2.11.
8. The SUT met the requirements with the exceptions noted in Table 1. DISA accepted the Vendor's POA&M and adjudicated these exceptions as minor.
9. The SUT supports CAS interfaces but they were not tested and are not included in this certification.
10. This optional requirement applies specifically to a Local Session Controller. The optional requirements for MSC, SSC, and ASAC were not tested and are not included in this certification.
11. This is a site requirement when the SUT is deployed to meet the power backup requirements and is a non-tested requirement.

(Table continues next page.)

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

LEGEND

AEI	AS-SIP End Instrument	MFS	Multifunction Switch
ASAC	Assured Services Admission Control	MG	Media Gateway
ASLAN	Assures Services Local Area Network	MGC	Media Gateway Controller
AS-SIP	Assured Services Session Initiation Protocol	MLPP	Multi-Level Precedence and Preemption
BRI	Basic Rate Interface	MSC	Master Session Controller
CAC	Common Access Card	NE	Network Element
CAS	Channel Associated Signaling	OCONUS	Outside the Continental United States
CCA	Call Connection Agent	PBAS	Precedence Based Assured Services
CR	Capability Requirement	PBX	Private Branch Exchange
DISA	Defense Information Systems Agency	PEI	Proprietary End Instrument
DoD	Department of Defense	POA&M	Plan of Action and Milestones
EI	End Instrument	PRI	Primary Rate Interface
EMS	Element Management System	PSTN	Public Switched Telephone Network
EO	End Office	SBC	Session Border Controller
ESC	Enterprise Session Controller	SC	Session Controller
FCAPS	Fault, Configuration, Accounting, Performance, and Security	SS	Softswitch
FR	Functional Requirement	SSC	Subtended Session Controller
IAD	Integrated Access Device	SUT	System Under Test
ID	identification	TA	Terminal Adapter
IP	Internet Protocol	TDM	Time Division Multiplexing
IPv6	Internet Protocol version 6	UC	Unified Capabilities
ISDN	Integrated Services Digital Network	UCR	Unified Capabilities Requirements
IWF	Interworking Function	VoIP	Voice over Internet Protocol
JITC	Joint Interoperability Test Command	VVoIP	Voice and Video over Internet Protocol

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

Component (See notes 1 and 2.)	**Release**	**Sub-component** (See notes 1 and 2.)	**HE, Env 1, 2, 3**	**Function**
Cisco Unified Communications Manager	14.0.1.11005-1	UCS ESXi version 6.5	HE, Env 1	UCM
Cisco Session Management Edition	14.0.1.11005-1	UCS ESXi version 6.5	HE	Session Management Edition
Cisco Unity Connection	14.0.1.10000-19	UCS ESXi version 6.5	HE, Env 1	Cisco Unity Connection
Instant Messaging & Presence Server	14.0.1.10000-16	UCS ESXi version 6.5	HE, Env 1	Instant Messaging & Presence Server
CMS	3.3.0.1	UCS ESXi version 6.5	HE, Env 1	MCU
Cisco Emergency Responder	14.0.1.10000-7	Not Applicable	HE, Env 1	E911 management system
Expressway Control Server	x12.6.4		Env 1, 2, 3	Expressway Control
Expressway Edge Server	x12.6.4		Env 1, 2, 3	Expressway Edge
Cisco UCCX	12.5SU1		HE, Env 1	Customer Premise Equipment
Cisco Finesse Web Application	12.5SU1		Env 1, 2, 3	
IWG on 4321 ISR, IWG on the 4461 ISR, IWG on 4331 ISR, IWG on 4351 ISR, IWG on 4431 ISR, **IWG on 4451-X ISR,** IWG on ASR 1001-X, **IWG on ASR 1002-X,** IWG on ASR 1004, IWG on ASR 1006, IWG on ASR 1006-X	IOS XE 17.03.03		HE, Env 1, 2	IWG
IWG on CSR-1000v	IOS XE 17.03.03		HE, Env 1, 2	IWG
SBC on 4321 ISR, SBC on the 4461 ISR, SBC on 4331 ISR, SBC on 4351 ISR, SBC on 4431 ISR, **SBC on 4451-X ISR,** SBC on ASR 1001-X, **SBC on ASR 1002-X,** SBC on ASR 1004, SBC on ASR 1006, SBC on ASR 1006-X	IOS XE 17.03.03		HE, Env 1, 2	SBC

(Table continues next page.)

Table 3-3. SUT Hardware/Software/Firmware Version Identification (continued)

Component (See notes 1 and 2.)	Release	Sub-component (See notes 1 and 2.)	HE, Env 1, 2, 3	Function
SBC on CSR-1000v	IOS XE 17.03.03	UCS ESXi version 6.5	HE, Env 1, 2	SBC
IWG/SBC on 4321 ISR, IWG/SBC on the 4461 ISR, IWG/SBC on 4331 ISR, IWG/SBC on 4351 ISR, IWG/SBC on 4431 ISR, **IWG/SBC on 4451-X ISR,** IWG/SBC on ASR 1001-X, **IWG/SBC on ASR 1002-X,** IWG/SBC on ASR 1004, IWG/SBC on ASR 1006, IWG/SBC on ASR 1006-X	IOS XE 17.03.03	Not Applicable	HE, Env 1, 2	IWG/SBC
IWG/SBC on CSR-1000v	IOS XE 17.03.03	UCS ESXi version 6.5	HE, Env 1, 2	IWG/SBC
4321 ISR, 4331 ISR, 4351 ISR, 4431 ISR, **4451-X ISR,** 4461 ISR	IOS XE 17.03.03	T1/E1 cards: **NIM-2MFT T1/E1**, NIM-1MFT-T1/E1, NIM-4MFT-T1/E1, NIM-8MFT-T1/E1	HE, Env 1, 2	Media Gateway
VG450	IOS XE 17.03.03	Service and Network interface modules: **SM-X-72FXS,** SM-X-8FXS/12FXO, SM-X-16FXS/2FXO, SM-X-24FXS/4FXO, **NIM-4FXSP,** NIM-2FXSP	Env 1, 2	Analog Voice Gateway
Media Termination Point on 4321 ISR Media Termination Point on 4331 ISR Media Termination Point on 4351 ISR Media Termination Point on 4431 ISR **Media Termination Point on 4451-X ISR** Media Termination Point on 4461 ISR	IOS XE 17.03.03		HE, Env 1, 2	Media Termination Point (MTP)
Jabber (Voice and Video Soft Client)	14.0.1.55914 (Build 305914) (Windows 10)		Env 1, 2, 3	IM&P, Voice, Video, Collaboration Soft Client
IP Phone 7811	sip78xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice)
IP Phone 7821	sip78xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice)
IP Phone 7841	sip78xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice)
IP Phone 7861	sip78xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice)
IP Phone 88XX	sip78xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone Tempest
Unified IP Phone 8811, 8811 Tempest	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
Unified IP Phone 8831 Conference Phone	sip88xx.14-0-1-0001-135	Not Applicable	Env 1, 2, 3	IP Phone (Voice and Video)
API EM-8831-xx	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
Unified IP Phone 8851 and 8851NR	sip88xx.12-7-1-0001-393		Env 1, 2, 3	IP Phone (Voice and Video)
API EM-8851–xx	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
CIS DTD-8851-01	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
Unified IP Phone 8841	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
API EM-8841–xx	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
API EL1-8841–xx	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
CIS DTD-8841-01	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
CIS DTD-8841T-01-L1	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
CIS DTD-8841-02	sip88xx.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
Unified IP Phone 8845	sip8845_65.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)

(Table continues next page.)

Table 3-3. SUT Hardware/Software/Firmware Version Identification (continued)

Component (See notes 1 and 2.)	Release	Sub-component (See notes 1 and 2.)	HE, Env 1, 2, 3	Function
Unified IP Phone 8861	sip88xx.14-0-1-0001-135	Not applicable	Env 1, 2, 3	IP Phone (Voice and Video)
Unified IP Phone 8865, 8865NR	sip8845_65.14-0-1-0001-135		Env 1, 2, 3	IP Phone (Voice and Video)
Unified IP Phone KEM Expansion module for 8800 series IP Phones	Not Applicable		Env 1, 2, 3	Expansion Module
Cisco IP Conference Phone 8832	sip88xx.14-0-1-0001-135		Env 1, 2, 3	Conference Phone
Cisco IP Conference Phone 8832 NR	sip88xx.14-0-1-0001-135		Env 1, 2, 3	Conference Phone
Cisco IP Conference Phone 7832	sip78xx.14-0-1-0001-135		Env 1, 2, 3	Conference Phone
Cisco Webex Room 55, Cisco Webex Room 55 Single NR, Cisco Webex Room 55 Dual, Cisco Webex Room 55 Dual NR, Cisco Webex Room 70G2 Single, Cisco Webex Room 70 G2 Single NR, Cisco Webex Room Dual, Cisco Webex Room 70 G2 Dual NR, Cisco Webex Room 70d, Cisco Webex Room 70s Endpoints	CE 9.14.6-cf0c4696851-2021-03-26		Env 1, 2, 3	Video Teleconference
Cisco Webex Room Kit, Cisco Webex Room Kit NR, Cisco Webex Room Kit Mini, Cisco Webex Room Kit Mini NR, Cisco Webex Room Kit Plus, Cisco Webex Room Kit Plus NR, Cisco Webex Room Kit Pro, Cisco Webex Room Kit Pro NR Endpoints	CE 9.14.6-cf0c4696851-2021-03-26		Env 1, 2, 3	Video Teleconference
Cisco Webex Board 55, Cisco Webex Board 55S, Cisco Webex Board 70, Cisco Webex Board 70S, and Cisco Webex Board 85S Endpoints	CE 9.14.6-cf0c4696851-2021-03-26		Env 1, 2, 3	Video Teleconference
Cisco Webex Desk Pro, Cisco Webex Desk Pro NR Endpoints	CE 9.14.6-cf0c4696851-2021-03-26		Env 1, 2, 3	Video Teleconference
Cisco Webex Room Panorama, Cisco Webex Room Panorama NR, Cisco Webex Room 70 Panorama, and Cisco Webex Room 70 Panorama NR endpoints	CE 9.14.6-cf0c4696851-2021-03-26		Env 1, 2, 3	Video Teleconference
Cisco Webex Room 70S NR and Cisco Webex Room 70D NR Endpoints	CE 9.14.6-cf0c4696851-2021-03-26		Env 1, 2, 3	Video Teleconference
GD vIPer	6.1.2.1 (See note 3.)		Env 1, 2, 3	Analog PSTN mode DSCD
GD IP vIPer	6.1.2.1 (See note 3.)		Env 1, 2, 3	SCCP and SIP modes DSCD

NOTE(S):
1. Components bolded and underlined were tested by JITC. The other components in the family series were not tested but are also certified for joint use. JITC certifies those additional components because they utilize the same software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.
2. A comprehensive list of supported hardware configurations can be found by selecting the "Cisco Unified Communications on the Cisco Unified Computing System" link at the following URL: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html.
3. Although the SUT was tested and is certified with this GD vIPer DSCD version, based on JITC analysis the SUT is also certified with other versions previously and currently listed on the DoDIN APL as interoperable for joint use with the SUT and denoted under a separate Tracking Number for the GD vIPEr DSCD.

(Table continues next page.)

Table 3-3. SUT Hardware/Software/Firmware Version Identification (continued)

LEGEND:			
API	Application Programming Interface	ISR	Integrated Services Router
APL	Approved Products List	IWG	Interworking Gateway
ASR	Aggregated Services Router	JITC	Joint Interoperability Test Command
CE	Collaboration Endpoint	KEM	Key Expansion Module
CIS	Cisco	LSC	Local Session Controller
CMS	Cisco Meeting Server	MCU	Multipoint Conference Unit
CSR	Cisco Cloud Services Router	MTP	Media Termination Point
DoDIN	Department of Defense Information Network	NR	No Radio
DSCD	DoD Secure Communications Device	PSTN	Public Switched Telephone Network
E911	Enhanced 911	SBC	Session Border Controller
Env	Environment (Type 1, 2 and 3)	SCCP	Skinny Call Control Protocol
ESC	Enterprise Session Controller	SIP/sip	Session Initiation Protocol
ESXi	Elastic Sky X infrastructure	SUT	System Under Test
GD	General Dynamics	UCCX	Unified Contact Center Express
HE	Head End	UCM	Unified Communications Manager
IM&P	Instant Messaging and Presence	UCS	Unified Computing System
IOS	Internetwork Operating System	URL	Uniform Resource Locator
IP	Internet Protocol	vIPer	Voice over IP Encryptor

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

System Name	Software Release		Function
Required Ancillary Equipment (Site-Provided)			
Public Key Infrastructure			
Syslog Server			
Test Network Components			
Avaya AS5300 Release 3.0 Service Pack 15	Avaya IP 1120, 1140	04.04.35	Voice EI
	Analog	NA	Voice EI
	GD IP/PSTN vIPer	6.1.1, 6.1.2.1	Secure Voice EI
REDCOM Sigma Release 2.2.8	Teo 7810	05.04.37	Voice EI
	Analog	NA	
	VVX 510	5.9.7.38223	Video EI
	VVX 610	5.9.7.38223	
	Plantronics Trio 8800	6.2.2.6-650033	
	Plantronics Trio 8500	7.0.1.1086	
	VVX 101, 150, 411, 450	5.9.7.32930	
	GD IP/PSTN vIPer	6.1.1, 6.1.2.1	Secure Voice EI
REDCOM HDX LSC Release 4.0AR5P6	VVX 510	5.9.7.38223	Video EI
	VVX 610	5.9.7.38223	
	Plantronics Trio 8800	6.2.2.6-650033	
	Plantronics G7500	3.3.2-286151	
	Plantronics X30	3.3.2-286151	
	Teo 7810	05.04.37	Voice AEI
	Analog	NA	Voice EI
	GD IP/PSTN vIPer	6.1.1, 6.1.2.1	Secure Voice EI
REDCOM SLICE LSC Release 4.0AR5P6	VVX 510	5.9.7.38223	Video AEI
	VVX 610	5.9.7.38223	
	Plantronics Trio 8800	6.2.2.6-650033	
	Plantronics X30	3.3.2-286151	
	Teo 7810	05.04.37	Voice EI
	GD IP/PSTN vIPer	6.1.1, 6.1.2.1	Secure Voice EI
Unify LSC Release 34.13 (V9R3.PS34.13)	Plantronics Real Presence Group Series 310	6.1.7-450056	Video AEI
	Teo 7810	05.04.37	Voice AEI
	GD IP/PSTN vIPer	6.1.1, 6.1.2.1	Secure Voice EI

(Table continues next page.)

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

System Name	Software Release		Function
Test Network Components (continued)			
NEC LSC Release 9.1	Plantronics Real Presence Group Series 300	6.1.7-450056	Video EI (H.323)
	Teo 7810/4101/4104	05.04.37	Voice EI
	GD IP/PSTN vIPer	6.1.1, 6.1.2.1	Secure Voice EI
Avaya Aura ESC 8.1	9608, 96x1	7.1.10.0r5	Voice AEI
	J100 Series Phones	R4.0.6.1.6.bin	Voice AEI
	IX Workplace VVoIP Soft Client	5.3.1.306	
Avaya CS2100 MFS Release SE09.1	Analog	NA	Voice EI
	BRI	NA	ISDN Voice EI

LEGEND:

AEI	AS-SIP End Instrument	LSC	Local Session Controller
AS	Application Server	NA	Not Applicable
AS-SIP	Assured Services Session Initiation Protocol	NEC	Network Enterprise Controller
BRI	Basic Rate Interface	PSTN	Public Switched Network
EI	End Instrument	SE	Succession Enterprise
ESC	Enterprise Session Controller	Syslog	System log
GD	General Dynamics	vIPer	Voice over IP Encryptor
HDX	High Density Exchange	VVoIP	Voice and Video over IP
IDSN	Integrated Services Digital Network	VVX	Voice and Video eXchange
IP	Internet Protocol		

Joint Interoperability Certification Revision History

Revision	Date	Approved By	Comments
N/A	8 October 2021	Bradley Clark	Original Joint Interoperability Certification.
1	18 November 2021	Elaine Macari	Amended the original certification memorandum as follows: • Multiple locations: Corrected IOS-XE to IOS XE. • In the memo, Table 4 (pages 4 through 6): o Line 3, Software Release: Corrected the version from 14.0.1.10000.20 **to** 14.0.1.11005-1. o Note 2 in table legend: Corrected the URL **from** https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-infrastructure.html **to** https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html. • In Enclosure 2, paragraph 2: o Multiple locations: – Removed references for the 2900 and 3900 IOS routers. – Revised the “Jabber for Windows” definition **from** “The Cisco Jabber for Windows provides the main workspace application for the ESC. It enhances productivity by unifying presence, IM, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one client on a user’s desktop. The Cisco Jabber for Windows delivers highly secure, clear, and reliable communications. It offers flexible deployment models, is built on open standards, and integrates with commonly used desktop applications. The Cisco Jabber client can also connect remotely to the ESC 21 through a remoter client GW or using a Domain Name System (DNS) federated session to connect through the Expressway Advanced Collaboration GW,” **to** “Provides the main workspace application for the ESC. It enhances productivity by unifying presence, IM, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one client on a user’s desktop. The Cisco Jabber for Windows delivers highly secure, clear, and reliable communications. It offers flexible deployment models, is built on open standards, and integrates with commonly used desktop applications. The Cisco Jabber client can also connect remotely to the ESC 21 through the Cisco Expressway Advanced Collaboration GW.” o Page 2-3, second paragraph: Corrected the URL **from** www.cisco.com/go/swonly **to** https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html. o Page 2-4, first paragraph: Corrected the URL **from** https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/ciscocollaboration-infrastructure.html **to** https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html. o In Enclosure 3, Page 3-7, Table 3-3 legend, Note 2: Corrected the URL **from** https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-infrastructure.html **to** https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html.

LEGEND:

DNS	Domain Name System	IOS	Internetwork Operating System
ESC	Enterprise Session Controller	N/A	Not Applicable
GW	Gateway	URL	Uniform Resource Locator
IM	Instant Messaging		