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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **4 Sep 12**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the T-Metrics, Inc.(TM)-2000, Consolidated Answering System (CAS) Version 6.0

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Defense Information Security Agency (DISA) Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The T-Metrics, Inc. (TM)-2000 Consolidated Answering System Version 6.0 is hereinafter referred to as the System Under Test (SUT). The SUT meets all of its critical interoperability requirements and is therefore certified for joint use within the Defense Information System Network (DISN) as a Customer Premise Equipment (CPE) specifically with any Cisco Unified Communications Manager (CUCM) Local Session Controller (LSC) or Avaya AS5300 LSC listed on the Unified Capabilities (UC) Approved Product List (APL). The SUT met the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d). No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that could affect interoperability, but no later than three years from the date of this memorandum.

3. This finding is based on interoperability testing conducted by JITC, review of the vendor's Letters of Compliance (LoC), and DISA Certifying Authority (CA) Recommendation of the Information Assurance (IA) configuration. Interoperability testing was conducted by JITC, Fort Huachuca, Arizona, from 28 May through 8 June 2012. Review of the vendor's LoC was completed on 21 May 2012. The DISA CA provided a positive Recommendation on 13 August 2012 based on the security testing completed by DISA-led IA test teams and published in a separate report, Reference (e). The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation. Enclosure 2 documents the test results and describes the tested network and system configurations including specified patch releases.

4. The interface, Capability Requirement (CR) and Functional Requirement (FR), and component status of the SUT are listed in Tables 1 and 2. The threshold CR/FRs for CPE are established by Section 5.2.1.2 of Reference (c) and were used to evaluate the interoperability of

the SUT. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

Table 1. SUT Interface Interoperability Status

Interface	Critical	UCR Reference	Threshold CR/FR (See note.)	Status
10Base-X	Yes	5.3.2.4.2	1-3	Certified
100Base-X	Yes	5.3.2.4.2	1-3	Certified
1000Base-X	No	5.3.2.4.2	1-3	Certified

NOTE: The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. The system under test does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements in order to be certified for that capability.

LEGEND:

CR	Capability Requirement	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements

Table 2. SUT CRs and FRs Status

CR/FR ID	Capability/Function	Applicability[1]	UCR Reference	Status
Product Interface Requirements				
1	Interfaces to LSC	Required	5.3.2.4.2	Met
Customer Premise Equipment Requirements				
2	MLPP in accordance with requirements listed in section 5.3.2.3.31.3	Conditional	5.2.1.2(1)	Met
	FCC Part 15/Part 68 and ACTA	Required	5.2.1.2(2)	Met
	Auto Answer mode settable to more than the equivalency of 4 ROUTINE rings	Conditional	5.2.12(3)	Not Tested[2]
	MLPP precedence call alerting	Conditional	5.2.1.2(4)	Not Tested[2]
	If configuration management and/or fault management are/is provided by the CPE device so that it can be managed by the ADIMSS or other management systems, the management information shall be provided by one or more serial or Ethernet interfaces.	Conditional	5.2.1.2(8)	Not Tested[2]
	Calls above ROUTINE placed to the SUT shall divert to a designated Directory Number.	Required	5.3.2.2.2.1.2.5	Met
IPv6 Requirements				
3	If a CPE has an IP interface, the CPE must be IPv6 capable. Use guidance in Table 5.3.5-4 for NA/SS	Required	5.3.5	Met[3]
Information Assurance				
4	Security	Required	5.4	Met[4]

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. This feature is conditional for a CPE and is not supported by the SUT.
3. Due to limitations in the test architecture IPv6 was unable to be tested across the network; however testing was conducted intra-enclave and compliance with IPv6 specifications was verified with vendor LoC.
4. Information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report, Reference (e).

Table 2. SUT CRs and FRs Status (continued)

LEGEND:

ACTA	Administrative Council for Terminal Attachments	IP	Internet Protocol
ADIMSS	Advanced Defense Switched Network (DSN) Integrated Management Support System	IPv6	Internet Protocol version 6
		LSC	Local Session Controller
CPE	Customer Premise Equipment	LoC	Letter of Compliance
CR	Capability Requirement	MLPP	Multi-Level Precedence and Preemption
DISA	Defense Information Systems Agency	NA/SS	Network Appliances and Simple Servers
FCC	Federal Communications Commission	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements
ID	Identification		

5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil.

6. The JITC point of contact is Capt Stéphane Arsenault, DSN 879-5269, commercial (520) 538-5269, FAX DSN 879-4347, or e-mail to Stephane.P.Arsenault.fm@mail.mil. JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 1134201.

FOR THE COMMANDER:

3 Enclosures a/s

for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

JITC Memo, JTE, Special Interoperability Test Certification of the T-Metrics, Inc.(TM)-2000, Consolidated Answering System (CAS) Version 6.0

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

ADDITIONAL REFERENCES

(c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 3," September 2011
(d) Joint Interoperability Test Command, "Unified Capabilities E911 Test Plan," Draft
(e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of T-Metrics Inc Consolidated Answering System (CAS) Version (v)6.0 (Tracking Number 1134201)," Draft

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. T-Metrics, Inc. (TM)-2000, Consolidated Answering System (CAS) Version 6.0; hereinafter referred to as the System Under Test (SUT).

2. SPONSOR. United States Air Force, Headquarters, Air Education and Training Command (HQ AETC/A6OI). Ricky Rider, 61 Main Circle, Suite 2, Randolph Air Force Base, Texas, 78150 e-mail: ricky.rider@randolph.af.mil.

3. SYSTEM POC. Mr. Bill Sandford, 4430 Stuart Andrew Boulevard, Charlotte, North Carolina 28217, e-mail: wsandford@tmetrics.com.

4. TESTER. Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

5. SYSTEM DESCRIPTION. The SUT allows calls placed from a remote location to be serviced by live agents at a consolidated (or central) location. Calls can be transferred by the agents at the centralized location because this system is designed so that most calls received at the remote bases are not forwarded or transferred to the consolidated location. Instead, the system at the remote base separates the elements of the original call into its audio component and its signaling component. The audio component is then connected from the remote base to the consolidated base using the Defense Switched Network (DSN) over a Primary Rate Interface (PRI) trunk or Signaling System Number 7 (SS7) and the signaling component is connected from the remote base to the consolidated base using an Internet Protocol (IP) network. The SUT is certified specifically with the Cisco Unified Communications manager (CUCM) Local Session Controller (LSC) and the Avaya AS5300 LSC listed on the Unified Capabilities (UC) Approved Products List (APL). The remote base's Time Division Multiplex (TDM) switch can be any DoD approved TDM-based or Session Initiation Protocol (SIP)-based switch.

Communication over the DSN network is treated like a DSN call with the same Multi-Level Precedence and Preemption (MLPP) priority as the call being serviced at the remote base. The communication over the IP network is encrypted with IP Security (IPSec) and uses a T-Metrics-defined protocol built to send only the information necessary to allow the agent in a consolidated location to handle the call.

Management Description. The SUT is managed directly by logging into an Agent Personal Computer (PC) using a Common Access Card (CAC) and Personnel Identification Number (PIN) associated to the local site's Public Key Infrastructure (PKI) and Active Directory (AD). Management access to the T-Metrics-2000 (TM-2000) Automatic Call Distribution (ACD) server and Remote SIP (RSIP) server is accomplished in a similar way and is only used for administrative functions for the system.

Agent PC. The Agent PC workstations are Government Furnished Equipment (GFE) Windows 7 Operating System (OS) PCs and run the Agent Module and Central

SIP Console (CSIP) client applications. The purpose of the Agent Module and CSIP applications are to allow the Agent PC to communicate to the TM-2000 Server that the agent has agreed to accept telephone calls from.

TM-2000 Automatic Call Distribution (ACD) Server. The TM-2000 ACD server combines TM-2000 multi-purpose platform and operator consoles into a CAS. The purpose of the CAS is to provide a bank of human agents at a specific location (Consolidated Answering Center) to answer calls at many remote bases that may no longer be staffed with human agents.

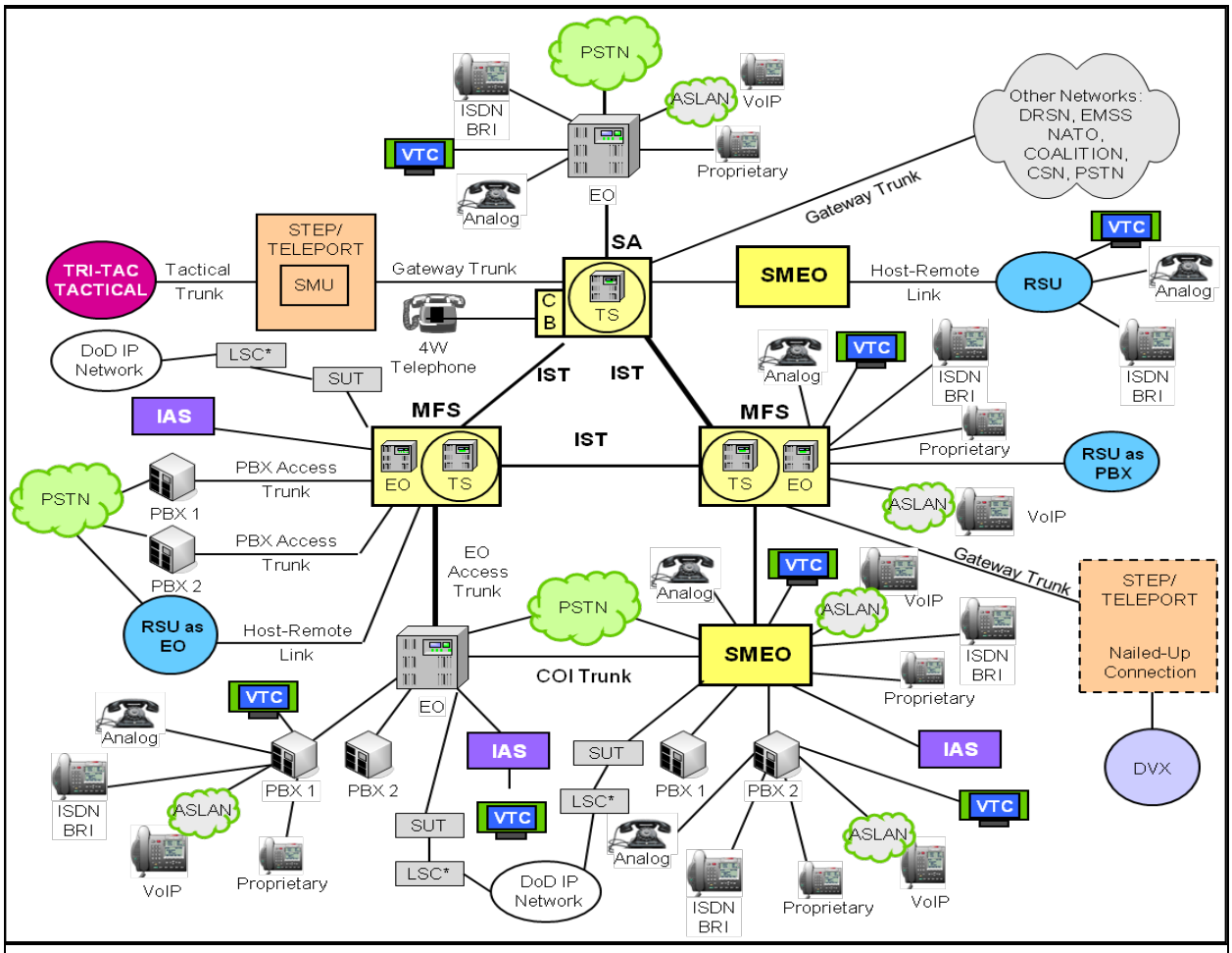
The key segments of the CAS are:

- Consolidated Answering Center - The home for all agents that answer and control the calls at the remote bases requiring assistance.
- Remote Bases - Various bases within the command that receive calls that require assistance from an agent trained in a particular skill.
- DSN - Carries the TDM-based audio between the remote bases and the CAS.
- The IP Network - Carries the status of indicators and displays from the remote bases to the Consolidated Answering Center and the actions taken by the agent (such as answer the call, release the call, transfer the call) from the Consolidated Answering Center to the remote bases. No audio or Voice over IP (VoIP) is transported over this channel.

The TM-2000 ACD server also accumulates performance statistics that are subsequently sent to an authorized terminal on the network.

RSIP Server. The T-Metrics RSIP server is the computer that receives SIP phone calls from the SIP-based switches at the hosted remote bases. The incoming SIP interfaces to the RSIP server use a separate Local Area Network (LAN) and Network Interface Card (NIC). These devices terminate the appropriate interface from the remote base switch. When an operator becomes available, the RSIP server uses another SIP interface to dial a headset connection to an operator at the consolidated answering center. The call control is managed by the IP connection between the RSIP and the ACD servers.

6. OPERATIONAL ARCHITECTURE. Figure 2-1 depicts the Defense Information System Network (DISN) Unified Capabilities notional operational architecture that the SUT may be used in.



NOTE: LSC* in the diagram denotes Avaya AS5300 or Cisco CUCM. The SUT is certified specifically with any Avaya AS5300 or Cisco CUCM LSC on the UC APL.

LEGEND:

4W	4-Wire
APL	Approved Products List
ASLAN	Assured Services Local Area Network
BRI	Basic Rate Interface
CB	Channel Bank
COI	Community of Interest
CSN	Canadian Switch Network
CUCM	Cisco Unified Communications Manager
DISN	Defense Information System Network
DoD	Department of Defense
DRSN	Defense Red Switch Network
DVX	Deployable Voice Exchange
EMSS	Enhanced Mobile Satellite System
EO	End Office
IAS	Integrated Access Switch
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
LSC	Local Session Controller
MFS	Multifunction Switch
NATO	North Atlantic Treaty Organization
PBX	Private Branch Exchange
PBX 1	Private Branch Exchange 1
PBX 2	Private Branch Exchange 2
PSTN	Public Switched Telephone Network
RSU	Remote Switching Unit
SA	Standalone
SMEO	Small End Office
SMU	Switched Multiplex Unit
STEP	Standardized Tactical Entry Point
SUT	System Under Test
Tri-Tac	Tri-Service Tactical Communications Program
TS	Tandem Switch
UC	Unified Capabilities
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing

Figure 2-1. DISN Unified Capabilities Notional Operational Architecture

7. INTEROPERABILITY REQUIREMENTS. The interface, Capability Requirements (CR) and Functional Requirements (FR), and other requirements for Customer Premise Equipments (CPEs) are established by Section 5.2.1.2 of Reference (c).

7.1 Interfaces. The SUT uses the interfaces shown in Table 2-1 to connect to the Global Information Grid network. This table shows the physical interfaces supported by the SUT and the associated standards.

Table 2-1. CPE Interface Requirements

Interface	Critical	UCR Reference	Criteria
10Base-X	Yes	5.3.2.4.2	Support minimum threshold CRs/FRs (1-3) and meet interface criteria for IEEE 802.3i.
100Base-X	Yes	5.3.2.4.2	Support minimum threshold CRs/FRs (1-3) and meet interface criteria for IEEE802.3u.
1000Base-X	No	5.3.2.4.2	Support minimum threshold CRs/FRs (1-3) and meet interface criteria for IEEE 802.3z or IEEE 802.3ab.

NOTES: The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. The system under test does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements in order to be certified for that capability.

LEGEND:

802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	FR	Functional Requirement
802.3i	10BaseT Mbps over twisted pair	Gbps	Gigabits per second
802.3u	Standard For Carrier Sense Multiple Access With Collision Detection At 100 Mbps	IEEE	Institute of Electrical and Electronics Engineers
CR	Capability Requirement	Mbps	Megabits per second
		SUT	System Under Test
		UCR	Unified Capabilities Requirements

7.2 CR and FR. CPEs have required and conditional features and capabilities that are established by Section 5.2.1 of the UCR. The SUT does not need to provide non-critical (conditional) requirements. If they are provided, they must function according to the specified requirements in order to be certified for that capability. The SUT's features and capabilities and its aggregated requirements in accordance with (IAW) the UCR CPE requirements are listed in Table 2-2. Detailed CR/FR requirements are provided in Table 3-1 of Enclosure 3.

Table 2-2. Customer Premise Equipment CRs and FRs

CR/FR ID	Capability/Function	Applicability (See note.)	UCR Reference
Product Interface Requirements			
1	Interfaces to LSC	Required	5.3.2.4.2

Table 2-2. Customer Premises Equipment CRs and FRs (continued)

CR/FR ID	Capability/Function	Applicability (See note.)	UCR Reference
Customer Premise Equipment Requirements			
2	MLPP in accordance with requirements listed in section 5.3.2.3.31.3	Conditional	5.2.1.2(1)
	FCC Part 15/Part 68 and ACTA	Required	5.2.1.2(2)
	Auto Answer mode settable to more than the equivalency of 4 Routine rings	Conditional	5.2.12(3)
	MLPP precedence call alerting	Conditional	5.2.1.2(4)
	If configuration management and or fault management are/is provided by the CPE device so that it can be managed by the ADIMSS or other management systems, the management information shall be provided by one or more derail or Ethernet interface	Conditional	5.2.1.2(8)
	Calls above Routine placed to the SUT shall divert to a designated Directory Number	Required	5.3.2.2.2.1.2.5
IPv6 Requirements			
3	If a CPE has an IP interface, the CPE must be IPv6 capable. Use guidance in Table 5.3.5-4 for NA/SS	Required	5.3.5-1
Information Assurance			
4	DISA STIGs	Required	5.3.2.34.9

NOTE: The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.

LEGEND:

ACTA	Administrative Council for Terminal Attachments	MLPP	Multilevel Precedence and Preemption
CPE	Customer Premises Equipment	IPv6	Internet Protocol version 6
CR	Capability Requirement	STIGs	Security Technical Implementation Guides
DISA	Defense Information Systems Agency	SUT	System Under Test
FCC	Federal Communications Commission	UCR	Unified Capabilities Requirements
FR	Functional Requirement		

7.3 Information Assurance (IA). Table 2-3 details the IA requirements applicable to the CPE products.

Table 2-3. CPE IA Requirements

Requirement	Applicability (See note.)	UCR Reference	Criteria
General Requirements	Required	5.4.6.2	Detailed requirements and associated criteria for CPE are listed in Reference (e).
Authentication	Required	5.4.6.2.1	
Integrity	Required	5.4.6.2.2	
Confidentiality	Required	5.4.6.2.3	
Non-Repudiation	Required	5.4.6.2.4	
Availability	Required	5.4.6.2.5	

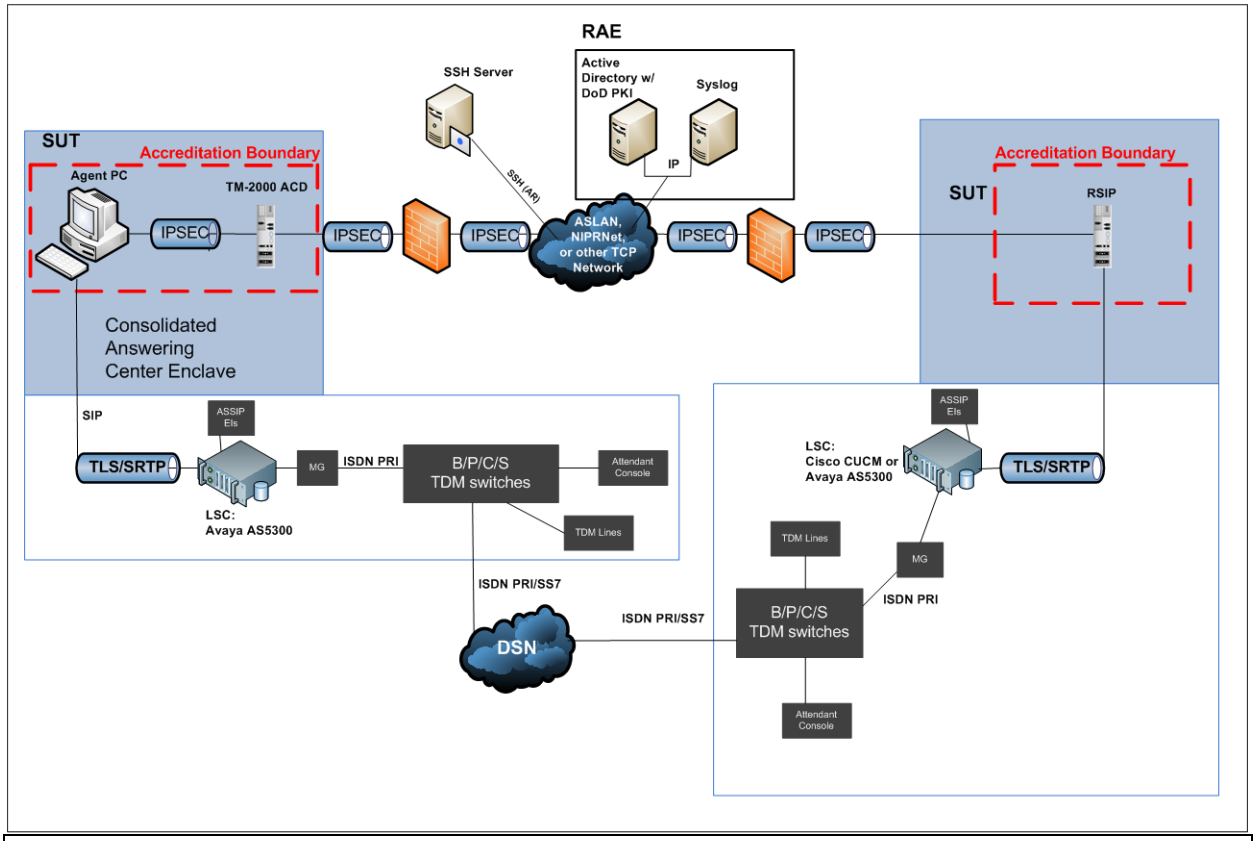
NOTE: The annotation of 'required' refers to a high-level requirement category of IA requirements from the UCR 2008, Change 3, Section 5.4. The detailed IA requirements are included in Reference (e).

LEGEND:

CPE	Customer Premises Equipment	UCR	Unified Capabilities Requirements
IA	Information Assurance		

7.4 Other. None

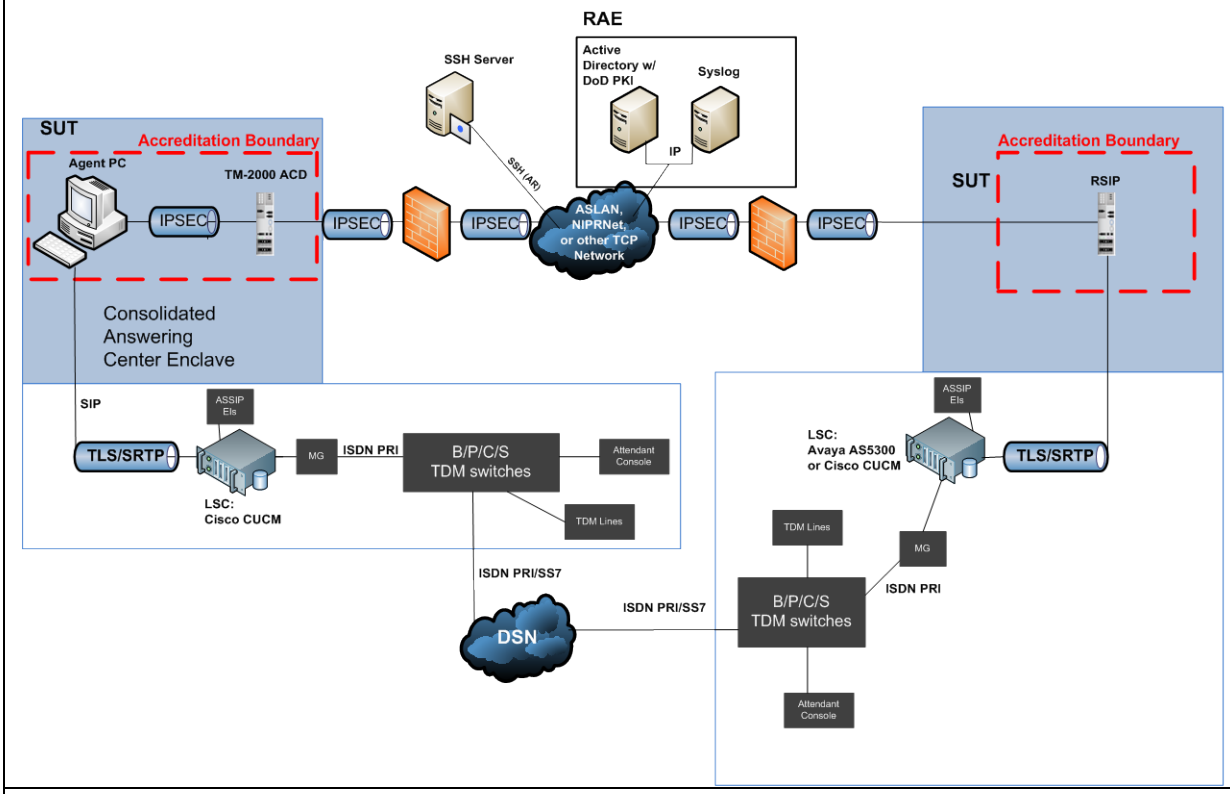
8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC, Fort Huachuca, Arizona, in a manner and configuration similar to that of a notional operational environment. Testing the system's required functions and features was conducted using the test configurations depicted in Figures 2-2 and 2-3. Figure 2-2 depicts the Avaya AS5300 LSC as the Consolidated Answering Center Enclave and the Cisco CUCM LSC as the Remote enclave. Figure 2-3 depicts the Cisco CUCM as the Consolidated Answering Center Enclave and the Avaya AS5300 LSC as the Remote Enclave.



LEGEND:

ACD	Automatic Call Distribution	MG	Media Gateway
ASLAN	Assured Services Local Area Network	PRI	Primary Rate Interface
ASSIP	Assured Services Session Initiation Protocol	RSIP	Remote SIP Server
B/P/C/S	Base, Post, Camp, Station	TDM	Time Division Multiplexing
CUCM	Cisco Unified Communications Manager	TLS	Transport Layer Security
DSN	Defense Switched Network	SSH	Secure Shell
IP	Internet Protocol	SRTP	Secure Real Time protocol
IPSEC	Internet Protocol Security	SUT	System Under Test
ISDN	Integrated Services Digital Network	TM	T Metrics
LSC	Local Session Controller		

Figure 2-2. Avaya AS5300 as Consolidated Answering Center Enclave



LEGEND:

ACD	Automatic Call Distribution	MG	Media Gateway
ASLAN	Assured Services Local Area Network	PRI	Primary Rate Interface
ASSIP	Assured Services Session Initiation Protocol	RSIP	Remote SIP Server
B/P/C/S	Base, Post, Camp, Station	TDM	Time Division Multiplexing
CUCM	Cisco Unified Communications Manager	TLS	Transport Layer Security
DSN	Defense Switched Network	SSH	Secure Shell
IP	Internet Protocol	SRTP	Secure Real Time protocol
IPSEC	Internet Protocol Security	SUT	System Under Test
ISDN	Integrated Services Digital Network	TM	T Metrics
LSC	Local Session Controller		

Figure 2-3. Cisco CUCM LSC as the Consolidated Answering Center Enclave

9. SYSTEM CONFIGURATIONS. Table 2-4 provides the system configurations and hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine its interoperability capability with UC switches noted in Table 2.4. The SUT is certified specifically with the Cisco CUCM and Avaya AS5300 LSCs listed on the UC APL.

Table 2-4. Tested System Configurations

System Name		Hardware/Software Release	
Avaya AS5300 LSC		Release 2.0 with Patch Bundle 23	
Cisco CUCM LSC		Release 8.6	
Required Ancillary Equipment		Active Directory	
		Public Key Infrastructure	
		SysLog Server	
SUT	T-Metrics Consolidated Answering System v6.0	**Component**	**Software/Firmware**
		Agent PC	Microsoft Windows 7 SP 1
			IE 9.0
			TMI DigiModule R4.0
			Agent Module v3.0
			Symantec Anti-Virus 11.0.6000.550
			CMSAC v6.0
			TotalHost v2.12
			Attachmate Reflection for Secure IT Client 7.2
		TM-2000 ACD Server	Windows 2008 R2
			IIS 7.5
			TMI DB v12.4.0
			ACD Controller v5.0
			Event Server v2.0
			TotalHost v2.12
			Attachmate Reflection for Secure IT Client 7.2
		RSIP Server	Windows 2008 R2
			TMI DigiModule R4.0
			TotalHost v2.12
			Attachmate Reflection for Secure IT Client 7.2

LEGEND:

ACD	Automatic Call Distribution	R	Release
AS	Application Server	RSIP	Remote SIP
CMSAC	Centralized Meridian Services Attendant Console	SIP	Session Initiation Protocol
CUCM	Cisco Unified Communications Manager	SP	Service Pack
IE	Internet Explorer	TM	T-Metrics
IIS	Internet Information Server	TMI	T-Metrics Interface
LSC	Local Session Controller	v	Version
PC	Personal Computer	WRQ	Write ReQuest

10. TESTING LIMITATIONS. Due to limitations in the test architecture, IPv6 was unable to be tested end-to-end inter-enclave. The SUT was; however, tested intra-enclave and the vendor submitted an IPv6 Letter of Compliance (LoC).

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for a CPE in accordance with UCR 2008, Change 3, section 5.2.1.2, and is certified for joint use with other network infrastructure products listed on the UC APL. Additional discussion regarding specific testing results is located in subsequent paragraphs.

11.1 Interfaces. The interface status of the SUT is provided in Table 2-5.

Table 2-5. SUT Interface Interoperability Status

Interface	Critical	UCR Reference	Threshold CR/FR (See note.)	Status
10Base-X	Yes	5.3.2.4.2	1-3	Certified
100Base-X	Yes	5.3.2.4.2	1-3	Certified
1000Base-X	No	5.3.2.4.2	1-3	Certified

NOTE: The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in
Enclosure 3. The system under test does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements in order to be certified for that capability.

LEGEND:

CR	Capability Requirement	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements

11.2 CR and FR. The SUT CR and FR status is depicted in Table 2-6. Detailed CR/FR requirements are provided in Enclosure 3, Table 3-1.

Table 2-6. SUT CR and FR Status

CR/FR ID	Capability/Function	Applicability[1]	UCR Reference	Status
Product Interface Requirements				
1	Interfaces to LSC	Required	5.3.2.4.2	Met
Customer Premise Equipment Requirements				
2	MLPP in accordance with requirements listed in section 5.3.2.3.31.3	Conditional	5.2.1.2(1)	Met
	FCC Part 15/Part 68 and ACTA	Required	5.2.1.2(2)	Met
	Auto Answer mode settable to more than the equivalency of 4 ROUTINE rings	Conditional	5.2.12(3)	Not Tested[2]
	MLPP precedence call alerting	Conditional	5.2.1.2(4)	Not Tested[2]
	If configuration management and/or fault management are/is provided by the CPE device so that it can be managed by the ADIMSS or other management systems, the management information shall be provided by one or more serial or Ethernet interfaces.	Conditional	5.2.1.2(8)	Not Tested[2]
	Calls above ROUTINE placed to the SUT shall divert to a designated Directory Number.	Required	5.3.2.2.2.1.2.5	Met
IPv6 Requirements				
3	If a CPE has an IP interface, the CPE must be IPv6 capable. Use guidance in Table 5.3.5-4 for NA/SS	Required	5.3.5	Met[3]
Information Assurance				
4	Security	Required	5.4	Met[4]

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. This feature is conditional for a CPE and is not supported by the SUT.
3. Due to limitations in the test architecture IPv6 was unable to be tested across the network; however testing was conducted intra enclave and compliance with IPv6 specifications was verified with vendor LoC.
4. Information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report, Reference (e).

Table 2-6. SUT CRs and FRs Status (continued)

LEGEND:

ACTA	Administrative Council for Terminal Attachments	IP	Internet Protocol
ADIMSS	Advanced Defense Switched Network (DSN) Integrated Management Support System	IPv6	Internet Protocol version 6
		LSC	Local Session Controller
CPE	Customer Premise Equipment	LoC	Letter of Compliance
CR	Capability Requirement	MLPP	Multi-Level Precedence and Preemption
DISA	Defense Information Systems Agency	NA/SS	Network Appliances and Simple Servers
FCC	Federal Communications Commission	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements
ID	Identification		

a. Product Interface Requirements. The UCR 2008, Change 3, section 5.3.2.4.2, states the physical interfaces between an LSC and its appliances shall be a 10/100/1000BaseT interfaces. The SUT interface shall support auto-negotiation even when the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard defines 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. The SUT met the requirements for the 10/100/1000BaseT interfaces through both testing and the vendor's LoC.

b. CPE Requirements

(1) The UCR 2008, Change 3, section 5.2.1.2(1), states all CPE devices that support MLPP shall do so in accordance with the requirements listed in Section 5.3.2.31.3, Multilevel Precedence and preemption, and shall not affect the DSN interface features and functions associated with line supervision and control. The SUT met this requirement with testing. Furthermore, all calls placed to the SUT above ROUTINE are appropriately routed to an alternate Directory Number (DN) or local Base/Post/Camp/Station attendant console.

(2) The UCR 2008, Change 3, section 5.2.1.2(2), states all DSN CPE, as a minimum, must meet the requirements of Part 15, and part 68 of the FCC Rules and Regulations, and the Administrative Council for Terminal Attachments. This requirement was met by the vendor's LoC.

(3) The UCR 2008, Change 3, section 5.2.1.2(3), states a device(s) that supports autoanswer shall have an autoanswer mode feature allowing the autoanswer mode to be set to a time more than the equivalency of four ROUTINE precedence ring intervals in accordance with Section 5.3.2.31.3, Multilevel Precedence and Preemption, before answer supervision is provided. This is a conditional requirement and is supported by the SUT; however, all calls above ROUTINE are diverted to the local attendant console or alternate DN.

(4) The UCR 2008, Change 3, section 5.2.1.2(4), states the device(s) that are required to support precedence calls above ROUTINE precedence shall respond properly to an incoming altering (ringing) precedence call cadence as described in

Section 5.3.2.6.1.1.1, UC Ringing Tones, Cadences, and Information Signals. This is a conditional requirement for a CPE device. All calls above ROUTINE are diverted to a local attendant console or alternate DN and therefore are not routed to the SUT.

(5) The UCR 2008, Change 3, section 5.2.1.2(8), states if Configuration Management and/or Fault Management are/is provided by the CPE device so that it can be managed by the Advanced Defense Switched Network Integrated Management Support System (ADIMSS) or other management system, then the management information shall be provided by one or more serial or Ethernet interface. This a conditional requirement and is not support by the SUT.

(6) The UCR 2008, Change 3, section 5.3.2.2.2.1.2.5, states that precedence calls above ROUTINE must be diverted to a designated DN. The SUT met this requirement through testing.

(7) The UCR 2008, Change 3, section 5.3.5, states if a CPE has an IP interface, the CPE must be IPv6 capable. Use guidance in Table 5.3.5-4 for Network Appliance/ Simple Server. This requirement was verified through the vendor's LoC and intra-enclave testing.

11.3 Information Assurance. Security is tested by DISA-led IA test teams and published in a separate report, Reference (e).

11.4 Other. None

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil.

SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The Customer Premises Equipment have required and conditional features and capabilities that are established by Section 5.2.1.2 of the Unified Capabilities Requirements (UCR) 2008, Change 3. The System Under Test (SUT) need not provide conditional requirements. If they are provided, they must function according to the specified requirements in order to be certified for that capability. The detailed Functional Requirements (FR) and Capability Requirements (CR) for Customer Premises Equipment are listed in Table 3-1. Detailed Information Assurance (IA) requirements are included in Reference (e) and are not listed below.

Table 3-1. Customer Premises Equipment Capability/Functional Requirements

ID	Requirement	UCR Reference	Required or Conditional
1	All CPE devices that support MLPP shall do so in accordance with the requirements listed in Section 5.3.2.31.3, Multilevel Precedence and Preemption, and shall not affect the DSN interface features and functions associated with line supervision and control.	5.2.1.2(1)	C
2	All DSN CPE, as a minimum, must meet the requirements of Part 15 and Part 68 of the FCC Rules and Regulations, and the Administrative Council for Terminal Attachments (ACTA).	5.2.1.2(2)	R
3	A device(s) that supports autoanswer shall have an "autoanswer" mode feature allowing the autoanswer mode to be set to a "time" more than the equivalency of four ROUTINE precedence ring intervals in accordance with Section 5.3.2.31.3, Multilevel Precedence and Preemption, before "answer" supervision is provided	5.2.1.2(3)	C
4	Devices that are required to support precedence calls above ROUTINE precedence shall respond properly to an incoming alerting (ringing) precedence call cadence as described in Section 5.3.2.6.1.1.1, UC Ringing Tones, Cadences, and Information Signals.	5.2.1.2(4)	C
5	A device(s) that can "out dial" DTMF and/or DP digits (automatic and/or manual) shall comply with the requirements as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 10 and be capable of outpulsing and interpretation of DTMF digits on outgoing or two-way trunks as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 15, and Table 5.2.1.2-1.	5.2.1.2(5)	C
6	Modems and facsimile machines shall be compatible with ITU and Telcordia standards, as applicable	5.2.1.2(6)	C
7	Facsimile devices, as a minimum, shall meet the requirements in accordance with applicable DISR standards.	5.2.1.2(7)	C
8	If Configuration Management and/or Fault Management are/is provided by the CPE device so that it can be managed by the ADIMSS or other management systems, then the management information shall be provided by one or more of the following serial or Ethernet interfaces: a. Serial interfaces shall be in accordance with one of the following standards: (1) ITU-T Recommendation V.35 (2) TIA-232-F (3) EIA-449-1 (4) TIA-530-A b. Ethernet interfaces shall be in accordance with IEEE 802.3-2002.	5.2.1.2(8)	C
9	As a minimum, the 911 and the E911 (tandem) emergency service shall have the capability to "hold" the originating subscriber or caller from releasing the call via the switch supervision interaction for line and trunk control by the "called-party" feature, in accordance with Telcordia Technologies GR-529-CORE. Additionally, the FCC regulations regarding 911 and E911 must be considered.	5.2.1.2(9)	C
10	The Customer Premises Equipment shall meet all of the IPv6 protocol requirements for NA/SS products in Section 5.3.5, IPv6 Requirements, including the requirements in Table 5.3.5-4, UC Network Appliances and Simple Servers (NA/SS).	5.3.5	R
11	Customer Premises Equipment shall meet the Information Assurance requirements of all applicable DISA STIGs.	5.4	R

Table 3-1. Customer Premises Equipment Capability/Functional Requirements (continued)

LEGEND:

ALI	Automatic Line Identification	IP	Internet Protocol
ACTA	Administrative Council for Terminal Attachments	IPv6	Internet Protocol version 6
B/P/C/S	Base/Post/Camp/Station	IEEE	Institute of Electrical and Electronics Engineers
C	Conditional	NA	Network Appliance
CPE	Customer Premises Equipment	R	Required
DISA	Defense Information Systems Agency	SS	Simple Servers
DP	Dial Pulse	STIGS	Security Technical Implementation Guides
DSN	Defense Switched Network	UC	Unified Capabilities
DTMF	Dual-Tone Multifrequency	UCR	Unified Capabilities Requirements
FCC	Federal Communications Commission		