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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **7 Jan 16**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Joint Interoperability Certification of the L-3 Secure Communications Interoperability Protocol (SCIP) Gateway (LSG) Release 1.4

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

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

Conditions of Certification. The L-3 SCIP Gateway Release 1.4, hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (b), and is certified for joint use as a Department of Defense Secure Communications Device (DSCD) with the conditions described in Table 1.

The SUT was tested with the Internet Protocol (IP) (Session Initiation Protocol [SIP]) interface connected to a Cisco Unified Communications Manager (UCM) for non-secure voice and connected to the Avaya CS2100 and Siemens Elektronisches Wählsystem Digital (EWSD) for secure (encrypted) voice. JITC analysis determined that the SUT is also certified for joint use on its secure interface side with any legacy Multifunction Switch (MFS), Small End Office (SMEO), or Private Branch Exchange (PBX), and any Unified Capabilities (UC) Local Session Controller (LSC), Multifunction Soft Switch (MFSS), or Wide Area Network (WAN) Soft Switch (SS) that is currently or was previously listed on the UC Approved Product List (APL) and included a certified Digital Transmission Link Level 1 (T1) Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) National ISDN 2 (NI2) interface. This certification expires upon changes that affect interoperability, but no later than three years from the date of the UC APL memorandum.

Desktop Review (DTR) 3 was requested to include an Out-of-Band Management (OOBM) port. See paragraph 4 for the test details.

Table 1. Conditions

Condition	Operational Impact	Remarks
UCR Waivers		
None.		
Conditions of Fielding		
The SUT disconnects all active calls at a configurable set time once every 24-hour clock cycle. The SUT must be deployed in accordance with the vendor's deployment guide to mitigate this issue.	Minor	See note 1.
Open Test Discrepancies		
The SUT does not support the ability to ignore redirect messages. The SUT is configured in accordance with the Operating System STIG to ignore IPv6 Redirects.	None	See note 2.

NOTE:
1. DISA had accepted and approved the vendor's POA&M and interim mitigations and adjudicated this discrepancy as having a minor operational impact. The original interim mitigation resulted in a 1 out of 24 chance that an active call will drop in less than 1 hour. The update to guarantee the 59-minute window for active calls was successfully tested with DTR 1, which updated the SUT from Release 1.4 to Release 1.5. This Release updates the SUT Non-Secure Voice Gateway from Release 1.41 to Release 1.43 and the SUT Secure (Encrypted) Voice Gateway from Release 1.2 to Release 1.21. DISA previously accepted and approved the vendor's POA&M and interim mitigations and adjudicated this discrepancy as having a minor operational impact.
2. DISA has adjudicated this issue as minor without POA&M.

LEGEND:

DISA	Defense Information Systems Agency	POA&M	Plan of Action and Milestones
DTR	Desktop Review	STIG	Security Technical Implementation Guide
IPv6	Internet Protocol version 6	SUT	System Under Test
NSA	National Security Agency	UCR	Unified Capabilities Requirements

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

Table 2. SUT Interface Status

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks
Interfaces			
Analog	1	Not Tested	
Basic Rate Interface (BRI)	1	Not Tested	
IP (SIP) 100 Mbps	1, 2, 3	Met	This interface is for the non-secure side. See note 2.
IP (AS-SIP)	1, 2, 3	Not Tested	
Primary Rate Interface (PRI)	1	Met	This interface is for the secure (encrypted) side. See note 3.

NOTES:
1. The UCR does not identify interface CR/FR applicability.
2. The SUT was tested and is certified for non-secure voice with an IP (SIP) interface connected to a Cisco Unified Communications Manager (UCM).
3. The SUT was tested and is certified on the secure (encrypted) side with the Avaya CS2100 and Siemens Elektronisches Wählsystem Digital (EWSD). JITC analysis determined that the SUT is also certified for joint use on its secure interface side with any legacy Multifunction Switch (MFS), Small End Office (SMEO), or Private Branch Exchange (PBX), and any Unified Capabilities (UC) Local Session Controller (LSC), Multifunction Soft Switch (MFSS), or Wide Area Network (WAN) Soft Switch (SS) that is currently or was previously listed on the UC Approved Product List (APL) and included a certified Digital Transmission Link Level 1 (T1) Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) National ISDN 2 (NI2) interface.

Table 2. SUT Interface Status (continued)

LEGEND:

AS-SIP	Assured Services Session Initiation Protocol	Mbps	Megabits per second
CRs	Capability Requirements	SIP	Session Initiation Protocol
DISA	Defense Information System Agency	SUT	System Under Test
FRs	Functional Requirements	UCR	Unified Capabilities Requirements
IP	Internet Protocol	VoSIP	Voice over Secure IP
JITC	Joint Interoperability Test Command		

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	Department of Defense Secure Communications Device (DSCD) (R)	3.8.2	Partially Met (See note 2.)
2	Differentiated Services Code Point Tagging Requirements (R)	7.2.1	Met
3	Internet Protocol version 6 Requirements (R)	Table 5.2-1	Partially Met (See notes 2, 3.)

NOTES:

1. The annotation of "required" refers to a high-level requirement category. The applicability of each sub-requirement is provided in Reference (c), Enclosure 3.
2. The SUT met the requirements with the exceptions noted in Table 1. DISA adjudicated these exceptions as minor.
3. The SUT was tested and met the requirements with IPv4. The SUT met the requirements for IPv6 with the vendor's LoC with the exception noted in Table 1.

LEGEND:

CR	Capability Requirement	IPv6	Internet Protocol version 6
DISA	Defense Information Systems Agency	LoC	Letters of Complaince
FR	Functional Requirement	R	Required
ID	Identification	SUT	System Under Test
IPv4	Internet Protocol version 4	UCR	Unified Capabilities Requirements

Table 4. SUT UC APL Product Summary

Product Identification			
Product Name	L-3 Secure Communications Interoperability Protocol (SCIP) Gateway (LSG)		
Software Release	1.5 (See note 1.)		
UC Product Type(s)	Department of Defense Secure Communications Device (DSCD)		
Product Description	The SUT was tested as a secure voice gateway with 24 channels that provided non-secure callers on a voice system to communicate with callers on a secure (encrypted) voice system that uses DSCD devices for de-encryption.		
Product Components (See note 2.)	**Component Name**	**Version**	**Remarks**
Secure voice gateway	L-3 SCIP Gateway	Red Side Release 1.43 Black Side Release 1.21	See notes 1, 3.
SNMP Management Terminal	SNMP Management Terminal (SMT)	Windows 7 SP1 SNMP Management Terminal v2.0.5.0	

NOTES:

1. The SUT was updated from Release 1.4 to Release 1.5 with DTR 1. This Release updates the SUT Non-Secure Voice Gateway from Release 1.41 to Release 1.43 and the SUT Secure (Encrypted) Voice Gateway from Release 1.2 to Release 1.21.
2. The detailed component and subcomponent list is provided in Reference (c), Enclosure 3.
3. The hardware was modified with DTR 3 to include Out-of-Band Management. The vendor modified the SUT removing the ability to manage the gateway from the Red traffic port and established a separate path for managing via OOBM. The modification adds an SNMP connection through an auxiliary Red Management Ethernet port located on the rear of the SUT Red SCIP Gateway subassembly providing an out-of-band management path for the SUT. There were no changes to the software.

LEGEND:

APL	Approved Products List	SNMP	Simple Network Management Terminal
DTR	Desktop Review	SUT	System Under Test
OOBM	Out-of-Band Management	UC	Unified Capabilities
SCIP	Secure Communications Interoperability Protocol		

Test Details. The extension of this certification is based upon DTR 3. The original certification, documented in Reference (c), is based on interoperability testing, review of the vendor's Letters of Compliance (LoC), DISA adjudication of open test discrepancy reports (TDRs), and DISA Certifying Authority (CA) Recommendation for inclusion on the UC APL. Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 26 December 2014 through 9 January 2015 using test procedures derived from Reference (d). Review of the vendor's LoC was completed on 12 December 2014. Patches were applied and Verification and Validation (V&V) testing was conducted on 13 March and 26 March 2015. DISA adjudication of outstanding TDRs was completed on 27 March 2015. The DISA CA provided a positive Recommendation based on the security testing completed by DISA-led IA test teams and the results published in a separate report, Reference (e).

This DTR was requested to include OOBM for connecting to the DISA Element Management System (EMS) - Data Communications Network (DCN) management network. The original certification includes in-band management via the Red traffic port. However, DISA requires an OOBM solution for connecting to the DISA EMS DCN. The vendor modified the SUT removing the ability to manage the gateway from the Red traffic port and established a separate path for OOBM. The modification adds an Simple Network Management Protocol (SNMP) connection through an auxiliary Red Management Ethernet port located on the rear of the LSG Red SCIP Gateway subassembly providing an OOBM path for the SUT. The SUT can be managed from any location on the network using authenticated SNMPv3. The SNMP Management Terminal (SMT) uses the SNMP MIB and presents the information in a context specialized for the SUT. The SMT is a site-provided management workstation running the Windows 7 Service Pack (SP) 1 Operating System (OS), and has the L-3 SMT configuration application loaded. Physical connection of the SMT to the gateway is over an Ethernet cable that is connected to the OOBM Ethernet port of the Red SCIP Gateway subassembly; the Black SCIP Gateway subassembly is not reachable from the secure network as a security measure.

The changes to provide the additional Ethernet port to provide OOBM are detailed in the following subparagraphs.

- The hardware was changed to add an Ethernet port to the rear of the Red SCIP Gateway subassembly using a panel mount connector attached to a previously blanked off port on the chassis.

- The hardware was changed for the internal wiring to connect the port to the master stack.

- The OS was reconfigured on the Master stack to enable the additional Ethernet port.

- The SNMP sub-agent was reconfigured on the Master stack to direct traffic to and from the additional Ethernet port.

- The OS was reconfigured on the Master stack to block SSH connections to the traffic Ethernet port.

- The OS was reconfigured on the Master stack to permit SSH connections to the management Ethernet port.

JITC determined IA Verification & Validation (V&V) testing was required. DISA-led IA test teams conducted IA testing on 17 and 18 December 2015. No changes to the system software or SUT version change was required for this DTR. The hardware and Master stack OS configuration must both be completed in new or existing chassis. The IA testing was conducted by DISA-led IA test teams and the results are published in a separate report, Reference (e). Therefore, JITC approves this DTR.

Additional Information. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified IP Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated information is available on the DISA UCCO website located at http://www.disa.mil/Services/Network-Services/UCCO.

Point of Contact (POC). The JITC point of contact is Capt. Soamva Duong, commercial telephone (520) 538-5269, DSN telephone 879-5269, FAX DSN 879-4347; e-mail address soamva.duong.fm@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTE (Capt. Soamva Duong) P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The UCCO tracking number for the SUT is 1426001.

FOR THE COMMANDER:

Enclosure a/s

for RIC HARRISON
Chief
Networks/Communications and UC Division

JITC Memo, JTE, Extension of the Joint Interoperability Certification of the L-3 Secure Communications Interoperability Protocol (SCIP) Gateway (LSG) Release 1.4

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

ADDITIONAL REFERENCES

(c) Joint Interoperability Test Command, Memo, JTE, "Joint Interoperability Certification of the L-3 Secure Communications Interoperability Protocol (SCIP) Gateway (LSG) Release 1.4," 9 April 2015
(d) Joint Interoperability Test Command, "SCIP Enabled DoD Secure Communications Device (DSCD) Test Procedures for Unified Capabilities Requirements (UCR) 2013 Errata 1," Draft
(e) Joint Interoperability Test Command, "Information Assurance (IA) Findings Summary (Phase I and Phase II) For L3 SCIP Gateway Release (Rel.) 1.4 (Tracking Number 1426001)," Draft