



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. Box 549
FORT MEADE, MARYLAND 20755-0549

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

30 Nov 11

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Special Interoperability Test Certification of the L-3 Communications Internet Protocol (IP) Secure Terminal Equipment (STE) Version 1.2.4

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 (h), see Enclosure 1 of the original certification memo (TN 0920506)

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

2. The L-3 Communications IP STE Version 1.2.4 is hereinafter referred to as the System Under Test (SUT). The SUT meets all of its critical interoperability requirements and is certified for joint use within the Defense Information System Network (DISN) as a Department of Defense (DoD) Secure Communications Device (DSCD). The SUT is certified with any Cisco CallManager (CCM) or Cisco Unified Communications Manager (CUCM) Private Branch Exchange or Local Session Controller and its associated gateway Internetwork Operating System (IOS) listed on the Unified Capabilities (UC) Approved Product List (APL) with one exception. The SUT when registered off of any CUCM and gateway with IOS 15.1(1) T experiences a high percentage of failed secure call attempts. This is associated with a problem with DSPWare which the vendor says they have no plans to fix. Therefore the SUT is not certified for joint use in the DISN with CUCM and any gateway with IOS 15.1(1)T. No other configurations, features, or functions, except those cited within this report, are certified by the JITC. This certification expires upon changes that could affect interoperability, but no later than three years from the date of Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG) accreditation.

3. The extension of this certification is based upon Desktop Review (DTR) 1. The original certification is based on interoperability testing conducted by JITC, review of the vendor's Letters of Compliance (LoC), adjudication of open test discrepancy reports by DISA and Theater Joint Tactical Network (TJTN), waiver of Internet Protocol version 6 (IPv6) requirements, National Security Agency (NSA) Type I Accreditation, and DSAWG accreditation. Interoperability testing of the SUT was conducted at JITC's Global Information Grid Network

Test Facility at Fort Huachuca, Arizona, from 8 March through 30 April 2010. Review of vendor's LoC was completed on 4 May 2010. The DISA and TJTN adjudication of outstanding test discrepancy reports was completed on 23 April 2010. The Office of the Secretary of Defense waived the IPv6 requirements on 27 September 2010 with the stipulation that the vendor provide a commitment to upgrade to IPv6 and demonstrate it during the Spiral 2 IPv6 Pilot test starting in the summer of 2011. The SUT NSA Type I accreditation was granted on 12 October 2010, as depicted in References (c) and (d). The DISA CA provided a positive recommendation on 23 November 2010 based on the security testing completed by DISA-led IA test teams and published in a separate report, Reference (e). Enclosure 2 of the original certification memo (TN 0920506) documents the test results and describes the tested network and system configurations. This DTR was requested to change the SUT software release from 1.2.4 to 1.2.5. Verification and Validation testing of this DTR was conducted by JITC from 8 through 12 August 2011. This updated software release 1.2.5 was applied to the SUT to fix open discrepancies with the CCM and CUCM listed on the UC APL. Specifically, a registration issue with CCM 4.3(2) and secure call failures with CUCM 8.0(2). Testing verified the updated software release 1.2.5 fixed the registration problem with the CCM. However, release 1.2.5 did not fix the secure call failure problem with CUCM and gateway with IOS 15.1(1)T. This DTR is approved with the caveat that the SUT is certified with any CCM and CUCM and its associated gateway IOS listed on the UC APL except for CUCM with IOS 15.1(1)T. No new IA findings or vulnerabilities were introduced with software release 1.2.5. Therefore, the original DISA CA recommendation applies to this DTR.

4. The interoperability test summary of the SUT is indicated in Table 1. The Unified Capabilities Requirement DSCD Interoperability Requirements are listed in Table 2. This interoperability test status is based on the SUT's ability to meet:

- a. Defense Switched Network (DSN) services for Network and Applications specified in Reference (f).
- b. DSCD interface and signaling requirements as specified in Reference (g) verified through JITC testing and/or vendor submission of LoC.
- c. DSCD Capability Requirements (CR)/Feature Requirements (FR) specified in Reference (g) verified through JITC testing and/or vendor submission of LoC.
- d. The overall system interoperability performance derived from test procedures listed in Reference (h).

Table 1. SUT Interoperability Test Summary

DSCD Interoperability Requirements			
Interface & Signaling	Critical	Status	Remarks
Ethernet 100BaseT (SCCP) (IEEE 802.3u)	Yes	Certified	The SUT met all Critical CRs and FRs with the following minor exceptions: The one-way latency was measured at 65 ms. ¹ The SUT does not support IPv6. ² The SUT does not set DSCP for any value 0 to 63. ³
Security	Yes	Certified ⁴	

Table 1. SUT Interoperability Test Summary (continued)

NOTES:			
1	The SUT had a measured one-way latency of 65 ms from handset to the T1 ISDN PRI gateway trunk egress, which did not meet this requirement. This discrepancy was adjudicated by DISA and the TJTN as having a minor operational impact.		
2	The Office of the Secretary of Defense waived the IPv6 requirements on 27 September 2010 with the stipulation that the vendor provide a commitment to upgrade to IPv6 and demonstrate it during the Spiral 2 IPv6 Pilot test starting in the summer of 2011.		
3	The SUT is hard coded with DSCP values of 0 for signaling and 40 for media. This discrepancy was adjudicated by DISA and the TJTN as having a minor operational impact with a POA&M. The vendor stated in their POA&M that this capability will be added in the next release of the SCCP IP STE in late 2011.		
4	Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (d).		
LEGEND:			
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	IP	Internet Protocol
APL	Approved Products List	IPv6	Internet Protocol version 6
CCM	Cisco CallManager	ISDN	Integrated Services Digital Network
CR	Capability Requirements	Mbps	Megabits per second
CUCM	Cisco Unified Communications Manager	POA&M	Plan of Action and Milestones
DISA	Defense Information Systems Agency	PRI	Primary Rate Interface
DSCD	Department of Defense (DoD) Secure Communications Device	SCCP	Skinny Client Control Protocol
DSCP	Differentiated Services Code Point	STE	Secure Terminal Equipment
FR	Feature Requirements	SUT	System Under Test
IEEE	Institute of Electrical and Electronics Engineers	T1	Digital Transmission Link Level 1 (1.544 Mbps)
IOS	Internetwork Operating System	TJTN	Theater Joint Tactical Network
		UC	Unified Capabilities

Table 2. DSCD UCR Interoperability Requirements

DSN Line Interface			
Interface	Critical	Requirements Required or Conditional	References
Ethernet 100BaseT (SCCP)	Yes	<ul style="list-style-type: none"> Type Approved by NSA (R) DSCDs that establish secure sessions on IP networks using FNBDT/SCIP shall satisfy all of the end point requirements described SCIP-215 and SCIP-216 (C) DSCD devices that use an IP interface shall meet the end instrument requirements as specified in UCR 2008 Change 1, Section, 5.3.2 (C) Shall go secure with at least an 85% call completion rate (R) Shall establish secure call within 60 seconds for duration of secure call (R) Shall operate in a network that has an end-to-end latency of up to 600 milliseconds (R) Maintain secure voice connection with MOS of 3.0 (R) Process new key with 95% rekey completion rate (R) Supports data and facsimile transmission rate of 9.6 kbps or better (C) 	<ul style="list-style-type: none"> UCR Section 5.2.5.2
Security		<ul style="list-style-type: none"> GR-815, STIGs, and DoDI 8510.bb (DIACAP) (R) 	<ul style="list-style-type: none"> UCR Section 3
LEGEND:			
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	FNBDT	Future Narrowband Digital Terminal
C	Conditional	GR	Generic Requirement
DIACAP	DoD Information Assurance Certification and Accreditation Process	GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security
DoD	Department of Defense	IP	Internet Protocol
DoDI	DoD Instruction	kbps	kilobits per second
DSCD	DoD Secure Communications Device	Mbps	Megabits per second
DSN	Defense Switched Network	MOS	Mean Opinion Score
		NSA	National Security Agency
		R	Required
		SCCP	Skinny Client Control Protocol
		SCIP	Secure Communications Internet Protocol
		STIGs	Security Technical Implementation Guides
		UCR	Unified Capabilities Requirements

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)

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the L-3 Communications Internet Protocol (IP) Secure Terminal Equipment (STE) Version 1.2.4

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), or <http://199.208.204.125> (SIPRNet). 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: ucco@disa.mil.

6. The JITC point of contact is Ms. Anita Mananquil, DSN 879-5164, commercial (520) 538-5164, FAX DSN 879-4347, or e-mail to anita.mananquil@disa.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 0922205.

FOR THE COMMANDER:

Enclosure a/s


for BRADLEY A. CLARK
Chief
Battlespace Communications Portfolio

Distribution (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ

U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68

Defense Information Systems Agency, GS23

ADDITIONAL REFERENCES

- (c) National Security Agency, “Information Assurance Directorate Certificate,” 21 September 2007
- (d) National Security Agency Secure Terminal Equipment (STE) Program Office, “Engineering Change Proposal,” 12 October 2010
- (e) Joint Interoperability Test Command, “Information Assurance (IA) Assessment of L-3 Communications Internet Protocol (IP) Secure Terminal Equipment (STE) Release (Rel.) 1.2.4 (Tracking Number 0922205),” 23 November 2010
- (f) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C, “Policy for Department of Defense Voice Services with Real Time Services (RTS),” 9 November 2007
- (g) Office of the Assistant Secretary of Defense, “Department of Defense Unified Capabilities Requirements 2008 Change 1,” 22 January 2010
- (h) Joint Interoperability Test Command, “Defense Switched Network Generic Switch Test Plan (GSTP), Change 2,” 2 October 2006