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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **21 Nov 12**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Special Interoperability Test Certification of the L-3 Communications Secure Terminal Equipment (STE) from Version 2.7 to Version 2.8

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 (g), see Enclosure

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

2. The L-3 Communications STE Version 2.7 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 Switched Network (DSN) as a Department of Defense (DoD) Secure Communications Device (DSCD). The SUT is certified with any switch in the DSN that offers a certified Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) National ISDN 2 (NI2) or analog loop-start interface with the following minor exceptions: The SUT is certified with the Alcatel-Lucent Class 5 Electronic Switching System (5ESS) and Siemens Elektronisches Wählsystem Digital (EWSD) with the analog interface only. 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 the original JITC certification memorandum (5 August 2010).

3. The extension of this certification is based upon Desktop Review (DTR) 1. The original certification is based on interoperability testing conducted by JITC and documented in Reference (c), DISA adjudication of open test discrepancy reports (TDRs), review of the vendor's Letters of Compliance (LoC), and National Security Agency (NSA) Type I 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. DISA adjudication of outstanding TDRs was completed on 23 April 2010. The SUT NSA Type I accreditation was granted on 23 June 2010, Reference (d). This DTR was requested to include Version 2.8. JITC determined that this would require Verification and Validation (V&V) testing. JITC conducted V&V testing from 5 through 13 November 2012. JITC testing verified that Version 2.8 did not introduce any new

discrepancies and two previous discrepancies documented in the subparagraphs below have been fixed and the TDRs have been closed. Therefore, JITC approves this DTR. The NSA Type I Accreditation for Version 2.8 was granted 10 July 2012, Reference (e).

a. After placing a call from the SUT to any other DSCD and initiating a secure call, the SUT randomly generated distortion on the receiving audio. The audio was degraded to the point that conversation was not possible and power-cycling the SUT was the only way to restore a usable audio path. This anomaly took place approximately 3 out of 640 calls and only when the SUT was in ISDN mode.

b. When the network was configured end-to-end ISDN with 600 milliseconds (ms) of one-way delay inserted to the transport, the SUT would not go secure in STE mode or the SUT would negotiate to Secure Communication Interoperability Protocol (SCIP) mode. The SUT in manual mode would go secure with up to 573 ms of delay, and the SUT in auto secure mode would go secure with up to 556 ms of delay.

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. 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 (CRs)/Feature Requirements (FRs) 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**
ISDN BRI NI 1/2 (ANSI T1.619a)	Yes	Certified	Met all critical CRs and FRs with the following minor exceptions: When the SUT is in ISDN mode, it does not ring at precedence above ROUTINE.[1] When the SUT is in ISDN mode, it does not support three-way conferencing when connected to the Siemens EWSD.[2] The SUT has a random one way audio distortion in secure mode when configured for ISDN mode.[3] The SUT does not support MLPP when connected to the Alcatel-Lucent 5ESS.[4] The SUT does not go secure with 600 ms of one way delay in STE mode over end-to-end ISDN.[5]
2-Wire Analog (Loop-Start)	Yes	Certified	Met all Critical CRs and FRs with the following minor exception: When the SUT is in PSTN mode, secure calls placed over a certified T1 CAS interface that has 437 ms to 440 ms of one-way delay will fail to go secure.[6]
Security	Yes	Certified	The SUT received NSA Type I Accreditation for Version 2.8 on 10 July 2012, Reference (e).

Table 1. SUT Interoperability Test Summary (continued)

NOTES:
1. When the SUT is in ISDN mode, all precedence calls above ROUTINE ring at the ROUTINE cadence. This discrepancy was adjudicated by DISA on 23 April 2010 as having a minor operational impact with the stipulation that the vendor provide a POAM. The vendor POAM states they will comply with Release 2.9 with a software update.
2. When the SUT is in ISDN mode, it does not support three-way conferencing when connected to the Siemens EWSD. Therefore, the SUT is not certified for use with the Siemens EWSD in ISDN mode. The SUT is certified for use with the Siemens EWSD using 2-wire analog; the operational impact is minor.
3. After placing a call from the SUT to any other DSCD and initiating a secure call, the SUT will randomly generate distortion on the receiving audio. When this occurs, the audio is degraded to the point that conversation is not possible. When this occurs, power-cycling the SUT is the only way to restore a usable audio path. This anomaly took place approximately 3 out of 640 calls and only when the SUT was in ISDN mode. This discrepancy was adjudicated by DISA on 23 April 2010 as having a minor operational impact. This anomaly did not occur on any of the approximately 100 calls made during testing for DTR 1 with release 2.8 loaded on the SUT.
4. When the SUT is in ISDN mode, it does not support MLPP when connected to the Alcatel-Lucent 5ESS. Therefore, the SUT is not certified for use with the Alcatel-Lucent 5ESS in ISDN mode. The SUT is certified for use with the Alcatel-Lucent 5ESS using 2-wire analog; the operational impact is minor.
5. When the network is configured end-to-end ISDN with 600 ms of one-way delay inserted to the transport (T1 PRI), the SUT does not go secure in STE mode or the SUT will negotiate to SCIP mode. The SUT in manual mode will go secure with up to 573 ms of delay, and the SUT in auto secure mode will go secure with up to 556 ms of delay. This discrepancy was adjudicated by DISA as having a minor operational impact with the stipulation that the vendor provide a POAM. The vendor POAM stated they will comply with Release 2.9 with a software update. This issue was corrected with release 2.8 when tested under DTR 1.
6. When the SUT is configured for PSTN mode and attempts a secure call over any T1 CAS interface that has 437 ms to 440 ms of one way delay, all secure call attempts fail to go secure. This discrepancy was adjudicated by DISA on 23 April 2010 as having a minor operational impact with the stipulation that the vendor provide a POAM. The vendor POAM states they will comply with Release 2.9 with a software update.

LEGEND:

5ESS	Class 5 Electronic Switching System	ms	milliseconds
ANSI	American National Standards Institute	NI1/2	National ISDN Standard 1 or 2
BRI	Basic Rate Interface	NSA	National Security Agency
CAS	Channel Associated Signaling	POAM	Plan of Action and Milestones
CRs	Capability Requirements	PRI	Primary Rate Interface
DISA	Defense Information Systems Agency	PSTN	Public Switched Telephone Network
DoD	Department of Defense	SCIP	Secure Communication Interoperability Protocol
DSCD	DoD Secure Communications Devices	SS7	Signaling System 7
EWSD	Elektronisches Wählsystem Digital	STE	Secure Terminal Equipment
FRs	Feature Requirements	SUT	System Under Test
ISDN	Integrated Services Digital Network	T1	Digital Transmission Link Level 1 (1.544 Mbps)
Mbps	Megabits per second	T1.619a	SS7 and ISDN MLPP Signaling Standard for T1
MLPP	Multi-Level Precedence and Preemption		

Table 2. DSCD UCR Interoperability Requirements

DSN Line Interface			
Interface	**Critical**	**Requirements Required or Conditional**	**References**
ISDN BRI NI 1/2 S/T	Yes	• DSCD devices shall meet the EI requirements as specified in UCR, Section 5.2.3 (R) - MLPP in accordance with UCR, section 5.2.2 (C) - FCC Part 68 and Part 15 compliance (R) - Auto-Answer mode settable to a "time" more than the equivalency of four ROUTINE precedence rings (C) - MLPP Precedence Call Alerting in accordance with UCR, section 5.2.4.5.1 (R) • DSCDs that use BRI shall meet the end instrument requirements specified in UCR, section 5.2.3.2.3 (ANSI T1.605-1991) (R) • Shall go secure with at least an 85% call completion rate (R) • Shall establish secure call within 60 seconds and maintain secure communications 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)	• UCR Section 5.2.5.2 • UCR Section 5.2.3.2 • UCR Section 5.2.3.2 • UCR Section 5.2.3.2 • UCR Section 5.2.3.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2

Table 2. DSCD UCR Interoperability Requirements

DSN Line Interface			
Interface	**Critical**	**Requirements Required or Conditional**	**References**
2-Wire Analog (Loop-Start)	Yes	• DSCD devices shall meet the EI requirements as specified in UCR, Section 5.2.3 (R) - MLPP in accordance with UCR, section 5.2.2 (C) - FCC Part 68 and Part 15 compliance (R) - Auto-Answer mode settable to a "time" more than the equivalency of four ROUTINE precedence rings (C) - MLPP Precedence Call Alerting in accordance with UCR, section 5.2.4.5.1 (R) - Out dial DTMF in accordance with UCR 2008, Section 5.2.4.4.2 (C) • DSCDs that use 2-wire analog shall meet the end instrument requirements specified in UCR, section 5.2.3.2.1 (TIA/EIA-470-B) (R) • Shall go secure with at least an 85% call completion rate (R) • Shall establish secure call within 60 seconds and maintain secure communications 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)	• UCR Section 5.2.5.2 • UCR Section 5.2.3.2 • UCR Section 5.2.3.2 • UCR Section 5.2.3.2 • UCR Section 5.2.3.2 • UCR Section 5.2.3.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2
Security	Yes	• Type Approved by NSA (R)	• UCR Section 5.2.5.2

LEGEND:

ANSI	American National Standards Institute	MLPP	Multi-Level Precedence and Preemption
BRI	Basic Rate Interface	MOS	Mean Opinion Score
C	Conditional	NI 1/2	National ISDN Standard 1 or 2
DoD	Department of Defense	NSA	National Security Agency
DSCD	DoD Secure Communications Device	R	Required
DSN	Defense Switched Network	S/T	4-Wire ISDN BRI Interface
DTMF	Dual-Tone Multi-frequency	T1.605	ISDN Basic Access Interface for S/T Reference Points and Layer 1 Specification
EIA	Electronic Industries Alliance		
EI	End Instrument	TIA	Telecommunications Industry Association
FCC	Federal Communications Commission	TIA/EIA-470-B	Performance and Compatibility Requirements for Telephone Sets with Loop Signaling
ISDN	Integrated Services Digital Network		
kbps	kilobits per second	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) 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). 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. All associated data is available on the DISA UCCO website located at http://www.disa.mil/ucco/.

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.l.mananquil.civ@mail.mil. JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 0920506.

FOR THE COMMANDER:

Enclosure a/s

for BRADLEY A. CLARK
Acting Chief
Battlespace Communications Portfolio

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

ADDITIONAL REFERENCES

(c) Joint Interoperability Test Command, Memo, JTE, "Special Interoperability Test Certification of the L-3 Communications Secure Terminal Equipment (STE) Version 2.7," 5 August 2010
(d) National Security Agency, "Information Assurance Directorate Certificate", 23 June 2010
(e) National Security Agency, "Information Assurance Directorate Certificate", 10 July 2012
(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