MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of L-3 Communications OMNIXi™ Secure Terminal 6.01

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 (f), see Enclosure 1

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 OMNIXi™ Secure Terminal 6.01 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). 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 this memorandum.

3. This finding is based on interoperability testing conducted by JITC, review of the vendor’s Letters of Compliance (LoC), DISA adjudication of open test discrepancy reports, 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 test discrepancy reports and review of the vendor’s LoC was completed on 23 April 2010. The security requirements for DSCD devices without Internet Protocol (IP) interfaces are satisfied with a NSA Type I Accreditation. The SUT NSA Type I accreditation was granted on 23 November 2010, Reference (c). Enclosure 2 documents the test results and describes the tested network and system configurations.

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:
JITC Memo, JTE, Special Interoperability Test Certification of L-3 Communications OMNIxi™ Secure Terminal 6.01

a. Defense Switched Network (DSN) services for Network and Applications specified in Reference (d).

b. DSCD interface and signaling requirements as specified in Reference (e) verified through JITC testing and/or vendor submission of LoC.

c. DSCD Capability Requirements (CRs)/ Feature Requirements (FRs) specified in Reference (e) verified through JITC testing and/or vendor submission of LoC.

d. The overall system interoperability performance derived from test procedures listed in Reference (f).

<table>
<thead>
<tr>
<th>Table 1. SUT Interoperability Test Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DSCD Interoperability Requirements</strong></td>
</tr>
<tr>
<td>Interface &amp; Signaling</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>2-Wire Analog (GR-506-CORE)</td>
</tr>
<tr>
<td>EIA-232 Serial</td>
</tr>
<tr>
<td>Security</td>
</tr>
</tbody>
</table>

**NOTES:**
1. When placing secure calls to and from the SUT and attempting to go to a non-secure state, the SUT will randomly fail to recognize when the connected POTS phone is placed on hook. When this occurs the SUT will no longer detect the onhook voltage and the only remedy is to power cycle the SUT. DISA adjudicated this as minor on 23 April 2010.
2. After initiating a successful secure call, the SUT displays the message “Call Terminated Please Hang UP”. When this occurs, calls could not be made to or from the SUT. The SUT required a power cycle to restore to a functional state. DISA adjudicated this as minor on 23 April 2010.

**LEGEND:**
- CRs: Capability Requirements
- DISA: Defense Information Systems Agency
- DoD: Department of Defense
- DSCD: DoD Secure Communications Devices
- EIA: Electronic Industries Alliance
- EIA-232: Standard for defining the mechanical and electrical characteristics for connecting Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) data communications devices
- FRs: Feature Requirements
- GR: Generic Requirement
- GR-506-CORE: LSSGR: Signaling for Analog Interfaces
- LSSGR: Local Access and Transport Area (LATA) Switching Systems Generic Requirements
- NSA: National Security Agency
- POTS: Plain Old Telephone Service
- SUT: System Under Test
## Table 2. DSCD UCR Interoperability Requirements

<table>
<thead>
<tr>
<th>Interface</th>
<th>Critical</th>
<th>Requirements Required or Conditional</th>
<th>References</th>
</tr>
</thead>
</table>
| 2 Wire Analog (GR-506-CORE) | Yes      | ● DSCD devices shall meet the End Instrument 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)  
- 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 5.2.5.2  
● UCR Section 5.2.5.2  
● UCR Section 5.2.5.2 |
| EIA-232 | No       | ● Supports data and facsimile transmission rate of 9.6 kbps or better (C) | ● UCR Section 5.2.5.2 |
| Security | Yes      | ● Type Approved by NSA (R) | ● UCR Section 5.2.5.2 |

**LEGEND:**
- C: Conditional
- DoD: Department of Defense
- DSCD: DoD Secure Communications Device
- DSN: Defense Switched Network
- EIA: Electronic Industries Alliance
- EIA-232: Standard for defining the mechanical and electrical characteristics for connecting Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) data communications devices
- FCC: Federal Communications Commission
- GR: Generic Requirement
- GR-506-CORE: LSSGR: Signaling for Analog Interfaces
- kbps: kilobits per second
- LSSGR: Local Access and Transport Area (LATA) Switching Systems Generic Requirements
- MOS: Mean Opinion Score
- NSA: National Security Agency
- Required
- R: Required
- UCR: Unified Capabilities Requirements

5. No detailed test report was developed in accordance with the Program Manager’s request. The 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](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](https://jit.fhu.disa.mil) (NIPRNet), or [http://199.208.204.226](http://199.208.204.226) (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at [http://jitc.fhu.disa.mil/tssi](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](mailto:ucco@disa.mil).
JITC Memo, JTE, Special Interoperability Test Certification of L-3 Communications OMNIxix™ Secure Terminal 6.01

6. The JITC point of contact is Mr. Joseph Roby, DSN 879-0507, commercial (520) 538-0507, FAX DSN 879-4347, or e-mail to joseph.roby@disa.mil. The JITC’s mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 0922206.

FOR THE COMMANDER:

[Signature]

RICHARD A. MEADOR
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,” 23 November 2010
(d) 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
(f) Joint Interoperability Test Command, “Defense Switched Network Generic Switch Test Plan (GSTP), Change 2,” 2 October 2006
CERTIFICATION TESTING SUMMARY

1. **SYSTEM TITLE.** L3 Communications OMNIxitm Secure Terminal Version 6.01; hereinafter referred to as the System Under Test (SUT).

2. **PROPOSENENT.** U.S. Army Communications-Electronics Command (CECOM) Theater Joint Tactical Networks (TJTN).

3. **PROGRAM MANAGER.** Mr. John Kahler, AMSEL-SE-WS-COM-EA, Building 1210 Rittko Avenue, Fort Monmouth, New Jersey, 07703, E-mail: john.kahler@us.army.mil.

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

5. **SYSTEM UNDER TEST DESCRIPTION.** The SUT is a secure device that provides Secure Communication Interoperability Protocol (SCIP) secure voice and secure data wireline connectivity between a locally connected device (e.g. an analog telephone or personal computer) and a remote, comparably-equipped device. The SUT supports Multi-Level Precedence and Preemption (MLPP). The SUT provides two RJ11 ports, one to connect to a local analog phone and one to connect to the Public Switched Telephone Network (PSTN). The SUT also provides a local serial data port to connect to a device to fill key material and to connect to a local computer for Secure Data applications. The SUT implements the Type 1 SCIP signaling and cryptography specifications as defined by the U.S. Government. The SUT is certified by the National Security Agency (NSA) to protect information classified Top Secret and below, using Type 1 encryption keys and algorithms for secure communications to a controlled group of user.

6. **OPERATIONAL ARCHITECTURE.** The Defense Switched Network (DSN) architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The DSN architecture, therefore, consists of several categories of switches, including Private Branch Exchanges (PBX)s. The Unified Capabilities Requirements (UCR) operational DSN Architecture is depicted in Figure 2-1.
**Figure 2-1. DSN Architecture**
7. **REQUIRED SYSTEM INTERFACES.** The SUT Interoperability Test Summary is shown in Table 2-1 and the Capability and Feature Requirements used to evaluate the interoperability of the SUT are indicated in Table 2-2. These requirements are derived from the UCR and verified through JITC testing and review of the vendor’s Letters of Compliance (LoC).

### Table 2-1. SUT Interoperability Test Summary

<table>
<thead>
<tr>
<th>Interface &amp; Signaling</th>
<th>Critical</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-Wire Analog (GR-506-CORE)</td>
<td>Yes</td>
<td>Certified</td>
<td>Met all Critical CRs and FRs with the following minor exceptions: The SUT fails to recognize when a connected POTS phone is placed on hook when going from a secure to non-secure state.&lt;sup&gt;1&lt;/sup&gt; After initiating a successful secure call, the SUT displays “Call Terminated Please Hang Up.”&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>EIA-232 Serial</td>
<td>No</td>
<td>Certified</td>
<td>Met all Critical CRs and FRs.</td>
</tr>
<tr>
<td>Security</td>
<td>Yes</td>
<td>Certified</td>
<td>The SUT received NSA Type I Accreditation on 23 November 2010, Reference (c).</td>
</tr>
</tbody>
</table>

**NOTES:**
1. When placing secure calls to and from the SUT and attempting to go to a non secure state, the SUT will randomly fail to recognize when the connected POTS phone is placed on hook. When this occurs the SUT will no longer detect the onhook voltage and the only remedy is to power cycle the SUT. DISA adjudicated this as minor on 23 April 2010.
2. After initiating a successful secure call, the SUT displays the message “Call Terminated Please Hang UP”. When this occurs, calls could not be made to or from the SUT. The SUT required a power cycle to restore to a functional state. DISA adjudicated this as minor on 23 April 2010.

**LEGEND:**
- **CRs** Capability Requirements
- **DISA** Defense Information Systems Agency
- **DoD** Department of Defense
- **DSCD** DoD Secure Communications Devices
- **EIA** Electronic Industries Alliance
- **EIA-232** Standard for defining the mechanical and electrical characteristics for connecting Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) data communications devices
- **FRs** Feature Requirements
- **GR** Generic Requirement
- **LSSGR** Local Access and Transport Area (LATA) Switching Systems Generic Requirements
- **NSA** National Security Agency
- **POTS** Plain Old Telephone Service
- **SUT** System Under Test

### Table 2-2. DSCD UCR Interoperability Requirements

<table>
<thead>
<tr>
<th>Interface</th>
<th>Critical</th>
<th>Requirements Required or Conditional</th>
<th>References</th>
</tr>
</thead>
</table>
| 2 Wire Analog (GR-506-CORE) | Yes | • DSCD devices shall meet the End Instrument 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)  
- 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 |
| EIA-232 | No | • Supports data and facsimile transmission rate of 9.6 kbps or better (C) | • UCR Section 5.2.5.2 |
| Security | Yes | • Type Approved by NSA (R) | • UCR Section 5.2.5.2 |
8. **TEST NETWORK DESCRIPTION.** The SUT was tested at JTC’s Global Information Grid Network Test Facility in a manner and configuration similar to that of the DSN operational environment. Testing of the SUT required functions and features was conducted using the test configurations depicted in Figures 2-2 through 2-9. Figures 2-2 through 2-8 simulate actual DoD operationally deployed network to strategic core network test configuration strings. The SUT was tested with other DSCD devices between the various test points denoted in each figure. Figure 2-9 depicts the test configuration used to test fax and modem calls with the SUT.
Figure 2-2. ADNS Composite Test Diagram
Figure 2-3. Air Force Composite Test Diagram
**Figure 2-4. CENTCOM Dual Hop Composite Test Diagram**
NOTE: The iDirect Modem without Satellite was available during testing, and satellite was simulated with an Adtech SX-12 Satellite Simulator.

Figure 2-5. CENTCOM Composite Test Diagram
NOTE: iDirect Modem w/ Satellite was not available during testing, and was simulated with an ANUE IP impairment device.

LEGEND:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4ESS</td>
<td>Class 4 Electronic Switching System</td>
</tr>
<tr>
<td>ASLAN</td>
<td>Assured Services Local Area Network</td>
</tr>
<tr>
<td>CAS</td>
<td>Channel Associated Signaling</td>
</tr>
<tr>
<td>CEU</td>
<td>Channel Encryption Unit</td>
</tr>
<tr>
<td>CS</td>
<td>Communication Server</td>
</tr>
<tr>
<td>DRSN</td>
<td>Defense Red Switch Network</td>
</tr>
<tr>
<td>DSCD</td>
<td>Department of Defense (DoD) Secure Communications Device</td>
</tr>
<tr>
<td>EC</td>
<td>Echo Canceller</td>
</tr>
<tr>
<td>EWSD</td>
<td>Elektronisches Wählsystem Digital</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>GW</td>
<td>Gateway</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>JCSE</td>
<td>Joint Communications Support Element</td>
</tr>
<tr>
<td>K</td>
<td>Kilobit</td>
</tr>
<tr>
<td>MFS</td>
<td>Multifunction Switch</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per second</td>
</tr>
<tr>
<td>NET</td>
<td>Network Equipment Technologies</td>
</tr>
<tr>
<td>PRI</td>
<td>Primary Rate Interface</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>SA</td>
<td>Satellite Access</td>
</tr>
<tr>
<td>STE</td>
<td>Secure Terminal Equipment</td>
</tr>
<tr>
<td>SUT</td>
<td>System Under Test</td>
</tr>
<tr>
<td>SWT</td>
<td>Secure Wireline Terminal</td>
</tr>
<tr>
<td>SX-12</td>
<td>Simulator, Data Link</td>
</tr>
<tr>
<td>TDMA</td>
<td>Digital Transmission Link Level 1 (1.544 Mbps)</td>
</tr>
<tr>
<td>T1</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>TX</td>
<td>Voice Exchange</td>
</tr>
</tbody>
</table>

Figure 2-6. JCSE DSCD Composite Test Diagram
Figure 2-7. USMC Composite Test Diagram
Figure 2-8. WIN-T Composite Test Diagram
9. SYSTEM CONFIGURATIONS. Table 2-2 provides the system configurations, hardware, and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine interoperability with a complement of DSN switches, Network Elements and comparable DSCD end instruments noted in Table 2-2. Table 2-2 lists the DSN switches and Network Elements which depict the tested configuration and is not intended to identify the only switches and Network Elements that are certified with the SUT. The SUT is certified with switching systems listed on the Unified Capabilities (UC) Approved Products List (APL) that offer the same certified interfaces.

Table 2-2. Tested System Configurations

<table>
<thead>
<tr>
<th>System Name</th>
<th>Software Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya CS2100 (MFS)</td>
<td>Succession Enterprise (SE) 09.1</td>
</tr>
<tr>
<td>Nokia-Siemens EWSD (MFS)</td>
<td>19d with Patch Set 46</td>
</tr>
<tr>
<td>Avaya S8710 (SMEO)</td>
<td>Communication Manager (CM) 4.0 (R014x.00.2.731.7: Super Patch 14419)</td>
</tr>
<tr>
<td>Avaya G3CSI (PBX 1)</td>
<td>Communication Manager (CM) 3.0 (R013.00.0.340.5: Patch 8893.1.0.7)</td>
</tr>
<tr>
<td>Cisco Unified CallManager (PBX 1)</td>
<td>Version 4.3(2) Service Release (SR) 1b, with Internetwork Operating System (IOS) Software Release 12.4(15) T7</td>
</tr>
<tr>
<td>Cisco Unified CallManager (PBX 1)</td>
<td>Version 7.1(2) with Internetwork Operating System (IOS) Software Release 12.4 (22) T2</td>
</tr>
<tr>
<td>REDCOM High Density Exchange (HDX) (SMEO)</td>
<td>Release 3.0A Revision 3, with Specified Patch Group 0 (3.0A R3P0)</td>
</tr>
<tr>
<td>Raytheon Channel Encryption Unit (CEU) (DSCD)</td>
<td>Release Version (v) 2.01.08 with LogiTel Mesh Router (MR) 1060 Release Version (v) 1.01.0205</td>
</tr>
<tr>
<td>L3 Communications STE (DSCD)</td>
<td>2.6 with KSV21</td>
</tr>
<tr>
<td>L3 Communications Omni Secure Wireline Terminal (DSCD)</td>
<td>5.07</td>
</tr>
<tr>
<td>L3 Communications STE (DSCD)</td>
<td>2.7 with KSV 21</td>
</tr>
<tr>
<td>NET Promina 800 and 400</td>
<td>4.x.2.02 Version 92.45</td>
</tr>
<tr>
<td>General Dynamics C4 Systems Sectéra® IP vIPer (DSCD)</td>
<td>1.0 Version 6.04</td>
</tr>
<tr>
<td>General Dynamics C4 Systems Sectera PSTN vIPer (DSCD)</td>
<td>2.14</td>
</tr>
<tr>
<td>General Dynamics C4 Systems Sectera (SWT)</td>
<td>12.5</td>
</tr>
</tbody>
</table>
Table 2-2. Tested System Configurations (continued)

<table>
<thead>
<tr>
<th>System Name</th>
<th>Software Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>NET VX900 (NE)</td>
<td>4.3.5 Version 55</td>
</tr>
<tr>
<td>Veraz DTX 600 (NE)</td>
<td>JITC022.1</td>
</tr>
<tr>
<td>SUT</td>
<td>Software Release</td>
</tr>
<tr>
<td>L-3 Communications OMNiX™</td>
<td>6.01</td>
</tr>
</tbody>
</table>

**LEGEND:**
- CS: Communication Server
- DSCD: Department of Defense (DoD) Secure Communications Device
- EWSD: Elektronisches Wählsystem Digital
- IP: Internet Protocol
- JTC: Joint Interoperability Test Command
- KSV: Key Operating Variable
- MFS: Multifunction Switch
- NET: Network Equipment Technologies
- PBX 1: Private Branch Exchange 1
- PSTN: Public Switched Telephone Network
- SED: Small End Office
- STE: Secure Terminal Equipment
- SUT: System Under Test

10. TESTING LIMITATIONS. None.

11. TEST RESULTS

a. Discussion

(1) The UCR, section 5.2.5.2, states that the enabled DSCD shall be only those that are Type Approved by the NSA and are listed on the NSA Secure Product Web site. Each DSCD must support at least one NSA approved secure protocol. If the DSCD supports more than one secure protocol, it must meet all the requirements for at least one of the secure protocols, and must minimally support the other protocols that are provided on the DSCD. The SUT received an NSA Type I approval for SCIP on 23 November 2010, which meets this requirement.

(2) The UCR, section 5.2.5.2, states that the enabled DSCD devices that use a 2-wire analog or Basic Rate Interface shall meet the End Instruments requirements as specified in UCR, section 5.2.3.2. The following End Instrument requirements were met by the SUT with testing or by LoC submitted by the vendor.

- All Customer Premise Equipment (CPE) devices that support MLPP shall do so in accordance with the requirements as listed in the UCR, section 5.2.2, and shall not affect the DSN interface features and functions associated with line supervision and control. The SUT supports MLPP interaction in accordance with this requirement.

- All DSN CPE, as a minimum, must meet the requirements of Part 15 and Part 68 of the Federal Communications Commission (FCC) Rules and Regulations, and the Administrative Council for Terminal Attachments (ACTA). This requirement was met by the SUT with an LoC submitted by the vendor.

(3) The UCR, section 5.2.5.2, states that a DSCD device that supports one of the required signaling modes shall interoperate with and establish secure session with other compatible devices with at least a 85 percent secure call completion rate. A total
of 4700 secure calls were placed with the SUT to other DSCD secure devices listed in Table 2-2 over the test configurations depicted in Figures 2-2 through 2-8 with a secure call completion rate of 87 percent, which meets this requirement.

(4) The UCR, section 5.2.5.2, states that the DSCD shall be capable of using the protocols provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call. A total of 4700 secure calls were placed over the test configurations depicted in Figures 2-2 through 2-8. All calls established a secure connection within 45 seconds and maintained calls until sessions were ended, which meets this requirement.

(5) The UCR, section 5.2.5.3, states that the DSCD shall operate in a network that has an end-to-end latency of up to 600 milliseconds (ms). A total of 4700 secure calls were placed over the test configurations depicted in Figures 2-2 through 2-8. The maximum end-to-end latency was 936 ms, which meets this requirement.

(6) The UCR, section 5.2.5.2, states that the DSCD shall achieve and maintain a secure voice connection with a minimum Mean Opinion Score (MOS) of 3.0. A SAGE 960B was used to measure MOS from the handset of the analog End Instrument connected to the SUT. A total of 4700 secure calls were placed over the test configurations depicted in Figures 2-2 through 2-8. MOS was measured between 4.0 and 4.02 in SCIP mode using the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) G.729 9.6 kilobits per second (kbps) Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-A CELP), which meets this requirement.

(7) The UCR, section 5.2.5.2, states that once connected to the rekey center, the DSCD shall obtain a new key and properly process that new key with a 95 percent rekey completion rate. The SUT rekey completion rate over test configurations depicted in Figures 2-2 through 2-8 was 100 percent for a total of 25 rekey calls attempted.

(8) The UCR, section 5.2.5.2, states that DSCD devices shall support a minimum data rate and facsimile (FAX) transmission rate of 9.6 kbps. A total of 15 secure data calls and 50 secure FAX calls were placed over the test diagrams depicted in Figure 2-9 with the SUT via the SUT’s serial interface. All calls were successful with a data rate of 9.6 kbps, which meets this requirement. In addition, 36 encryption key data transfers using Data Transfer Devices were placed with the SUT at a data rate of 9.6 kbps. All data transfers were successful with a data rate of 9.6 kbps, which meets this requirement.

(9) Security. The security requirements for DSCD devices without Internet Protocol (IP) interfaces are satisfied with a NSA Type I accreditation. The SUT NSA Type I accreditation was granted on 23 November 2010, which meets this requirement.

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager’s request. The 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), 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.