



DEFENSE INFORMATION SYSTEMS AGENCY
 JOINT INTEROPERABILITY TEST COMMAND
 P.O. BOX 12798
 FORT HUACHUCA, ARIZONA 85670-2798

IN REPLY REFER TO: Networks and Transport Division (JTE)

13 May 05

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of Real Time Monitors, Inc. Switch Expert™ with Software Release 5.5

References: (a) DOD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
 (b) CJCSI 6212.01C, "Interoperability and Supportability of Information Technology and National Security Systems," 20 November 2003

1. References (a) and (b) establish the Defense Information Systems Agency, Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification. Additional references are provided in enclosure 1.
2. Real Time Monitors, Inc. Switch Expert™ with Software Release 5.5, hereinafter referred to as the system under test (SUT), meets the interface and functional requirements and is certified for joint use within the Defense Switched Network (DSN) specifically with the Nortel Networks switches listed in table 1. The SUT met the interface and functional requirements for customer premise equipment devices set forth in appendix 7 of reference (c). Testing was conducted using test procedures derived from reference (d). This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.

Table 1. SUT Interoperable Switches

Switch	NM Functional Requirements	Interface
MSL-100	- Fault Management - Performance Management - Automated Message Accounting - Configuration Management	EIA-232
Meridian 1 Options 11C, 11C Mini		EIA-232
Meridian 1 Options 51C, 61C, and 81C		EIA-232
LEGEND: EIA - Electronic Industries Alliance MSL - Meridian Switching Load NM - Network Management SUT - System Under Test		

3. This certification is based on interoperability testing conducted by JITC at the Global Information Grid Network Test Facility, Fort Huachuca, AZ, from 16 through 18 February 2005. Review and approval of vendor Letters of Compliance was completed on 22 February 2005 and

product comparison and data review was completed on 11 March 2005. The Certification Testing Summary (enclosure 2) documents the test results and describes the test configuration. Users should verify interoperability before deploying the SUT in an environment that varies significantly from that described.

4. The Functional Requirements used to evaluate the interoperability of the SUT and the interoperability statuses are indicated in table 2.

Table 2. SUT Functional Requirements and Interoperability Status

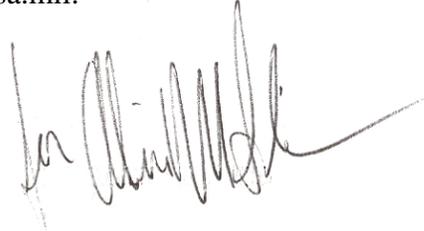
Interfaces	Critical	Certified	Functional Requirements	Met	GSCR Paragraph																																
Ethernet TCP/IP IEEE 802.3 (10BaseT)	No ¹	Yes	Fault Management (C)	Met	A.7.5																																
			Performance Management (C)	Met																																	
Ethernet TCP/IP IEEE 802.3.u (100BaseTX)	No ¹	Yes	Automated Message Accounting (C)	Met																																	
			Configuration Management (C)	Met																																	
EIA-232 Serial	No ¹	Yes	Security in accordance with DITSCAP (R)	Not Tested ²	A.7.6.5																																
<p>LEGEND:</p> <table border="0"> <tr> <td>802.3</td> <td>- IEEE standard for carrier sense multiple access with collision detection at 10 Mbps</td> <td>EIA</td> <td>- Electronic Industries Alliance</td> </tr> <tr> <td>802.3u</td> <td>- IEEE standard for carrier sense multiple access with collision detection at 100 Mbps</td> <td>IEEE</td> <td>- Institute of Electrical and Electronics Engineers, Inc.</td> </tr> <tr> <td>10BaseT</td> <td>- 10 Mbps (Baseband Operation, Twisted Pair) Ethernet</td> <td>GSCR</td> <td>- Generic Switching Center Requirements</td> </tr> <tr> <td>100BaseTX</td> <td>- 100 Mbps Ethernet over Category 5 Twisted Pair Copper</td> <td>Mbps</td> <td>- Megabits per second</td> </tr> <tr> <td>A</td> <td>- Appendix</td> <td>R</td> <td>- Required</td> </tr> <tr> <td>C</td> <td>- Conditional</td> <td>SUT</td> <td>- System Under Test</td> </tr> <tr> <td>DISA</td> <td>- Defense Information Systems Agency</td> <td>TCP/IP</td> <td>- Transmission Control Protocol/Internet Protocol</td> </tr> <tr> <td>DITSCAP</td> <td>- Department of Defense Information Technology Security Certification and Accreditation Process</td> <td></td> <td></td> </tr> </table> <p>NOTES:</p> <p>1 The Network Management requirements can be met via one of the following interfaces: Ethernet/TCP/IP (IEEE 802.3), Serial/Asynchronous (EIA-232), or Serial/Synchronous (X.25 and/or BX.25 variant)</p> <p>2 DITSCAP information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.</p>						802.3	- IEEE standard for carrier sense multiple access with collision detection at 10 Mbps	EIA	- Electronic Industries Alliance	802.3u	- IEEE standard for carrier sense multiple access with collision detection at 100 Mbps	IEEE	- Institute of Electrical and Electronics Engineers, Inc.	10BaseT	- 10 Mbps (Baseband Operation, Twisted Pair) Ethernet	GSCR	- Generic Switching Center Requirements	100BaseTX	- 100 Mbps Ethernet over Category 5 Twisted Pair Copper	Mbps	- Megabits per second	A	- Appendix	R	- Required	C	- Conditional	SUT	- System Under Test	DISA	- Defense Information Systems Agency	TCP/IP	- Transmission Control Protocol/Internet Protocol	DITSCAP	- Department of Defense Information Technology Security Certification and Accreditation Process		
802.3	- IEEE standard for carrier sense multiple access with collision detection at 10 Mbps	EIA	- Electronic Industries Alliance																																		
802.3u	- IEEE standard for carrier sense multiple access with collision detection at 100 Mbps	IEEE	- Institute of Electrical and Electronics Engineers, Inc.																																		
10BaseT	- 10 Mbps (Baseband Operation, Twisted Pair) Ethernet	GSCR	- Generic Switching Center Requirements																																		
100BaseTX	- 100 Mbps Ethernet over Category 5 Twisted Pair Copper	Mbps	- Megabits per second																																		
A	- Appendix	R	- Required																																		
C	- Conditional	SUT	- System Under Test																																		
DISA	- Defense Information Systems Agency	TCP/IP	- Transmission Control Protocol/Internet Protocol																																		
DITSCAP	- Department of Defense Information Technology Security Certification and Accreditation Process																																				

5. 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>.

JITC Memo, JTE, Special Interoperability Test Certification of Real Time Monitors, Inc. Switch Expert™ with Software Release 5.5

6. The JITC point of contact is Mr. John Hooper, DSN 879-5041, commercial (520) 538-5041, FAX DSN 879-4347, or e-mail to John.Hooper@disa.mil.

FOR THE COMMANDER:



RICHARD A. MEADOR
Chief
Networks and Transport Division

2 Enclosures a/s

Distribution:

Joint Staff J6I, Room-1E565, Pentagon, Washington, DC 20318-6000

Joint Interoperability Test Command, Washington Operations Division, NSWC, ATTN: JT1,
Building 900, 101 Strauss Avenue, Indian Head, MD 20640-5035

Defense Information Systems Agency, GIG Enterprise Services Engineering Directorate,
NETCENTRICITY, REQUIREMENTS, ANALYSIS & ASSESSMENTS BRANCH, ATTN:
GE333, Rm. 244, 5600 Columbia Pike, Falls Church, VA 22041-2770

Defense Information Systems Agency, GIG-Combat Support Directorate, DSN SYSTEMS
MANAGEMENT BRANCH, ATTN: GS235, Rm. 5W248A, 5275 Leesburg Pike, Falls
Church, VA 22041

Office of Chief of Naval Operations (N61C22), CNON6/7, 2000 Navy Pentagon, Washington,
DC 20350

Headquarters US Air Force, AF/XICC, 1250 Pentagon, Washington, DC 20330-1250

Department of the Army, Office of the Secretary of the Army, G-6/ASA (ALT), ATTN:
ASAALT (SAAL-SSI), 103 Army Pentagon, Washington, DC 20310-0103

US Marine Corps (C4ISR), MARCORSYSCOM, 2200 Lester Street, Quantico, VA 22134

DOT&E, Strategic and C3I Systems, 1700 Defense Pentagon, Washington, DC 20301-1700

US Coast Guard, COMDT/G-SCE (C4), 2100 2nd Street SW, Washington, DC 20593

Office of Assistant Secretary of Defense, OASD(NII)/DoD CIO, Crystal Mall 3, 7th Floor, Suite
700, 1931 Jefferson-Davis Hwy, Arlington, VA 22202

Office of Under Secretary of Defense, OUSD(AT&L), Room 3E144, 3070 Defense Pentagon,
Washington, DC 20301

US Joint Forces Command, J6I, C4 Plans and Policy, 1562 Mitscher Ave, Norfolk, VA 23551-
2488

Defense Intelligence Agency, ATTN: DS-CIO, Bldg 6000, Bolling AFB, Washington, DC
20340-3342

National Security Agency, ATTN: DT, Suite 6496, 9800 Savage Road, Fort Meade, MD
20755-6496

Commander, Defense Information Systems Agency (DISA), ATTN: GS23 (Mr. Osman), Room
5w23, 5275 Leesburg Pike (RTE 7), Falls Church, VA 22041

ADDITIONAL REFERENCES

- (c) Defense Information Systems Agency, "Department of Defense Voice Networks Generic Switching Center Requirements (GSCR)," 8 September 2003
- (d) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP)," 23 April 2004

CERTIFICATION TESTING SUMMARY

- 1. SYSTEM TITLE.** Real Time Monitors, Inc. Switch Expert™ with Software Release 5.5, hereinafter referred to as the system under test (SUT).
- 2. PROPONENT.** Defense Information Systems Agency (DISA).
- 3. PROGRAM MANAGER.** Mr. Howard Osman, GS23, Room 5W23, 5275 Leesburg Pike, Falls Church, VA 22041, e-mail: Howard.Osman@disa.mil.
- 4. TESTER.** Joint Interoperability Test Command (JITC), Ft. Huachuca, AZ.
- 5. SYSTEM UNDER TEST DESCRIPTION.** The SUT is an Internet Protocol based client/server network element monitoring application that utilizes Advanced Encryption Standard (AES). The SUT is used to simultaneously monitor multiple switching systems in real-time and provide point and click access to call detail records, system events and traffic analysis reports. The SUT is configured in a host/remote relationship; this configuration enables the SUT remotes to relay locally processed call detail records and system events to its host. If network connectivity is lost between the SUT host and remote, the remote will automatically operate in a fully functional standalone server mode until the network resources are restored. In addition to monitoring all system events, the SUT monitors and detects loop contact closures from external devices such as system alarm status, environmental alarms, switch room access etc. The SUT is interoperable solely with Nortel Networks Meridian Switching Load (MSL)-100 and Meridian 1 switches as shown in table 2-1.

Table 2-1. SUT Interoperable Switches

Switch	NM Functional Requirements	Interface
MSL-100	<ul style="list-style-type: none"> - Fault Management - Performance Management - Automated Message Accounting - Configuration Management 	EIA-232
Meridian 1 Options 11C, 11C Mini		EIA-232
Meridian 1 Options 51C, 61C, and 81C		EIA-232
LEGEND: EIA - Electronic Industries Alliance MSL - Meridian Switching Load NM - Network Management SUT - System Under Test		

- 6. OPERATIONAL ARCHITECTURE.** The Generic Switching Center Requirements (GSCR) Defense Switched Network (DSN) architecture in figure 2-1 depicts the relationship of the SUT to the DSN switches.

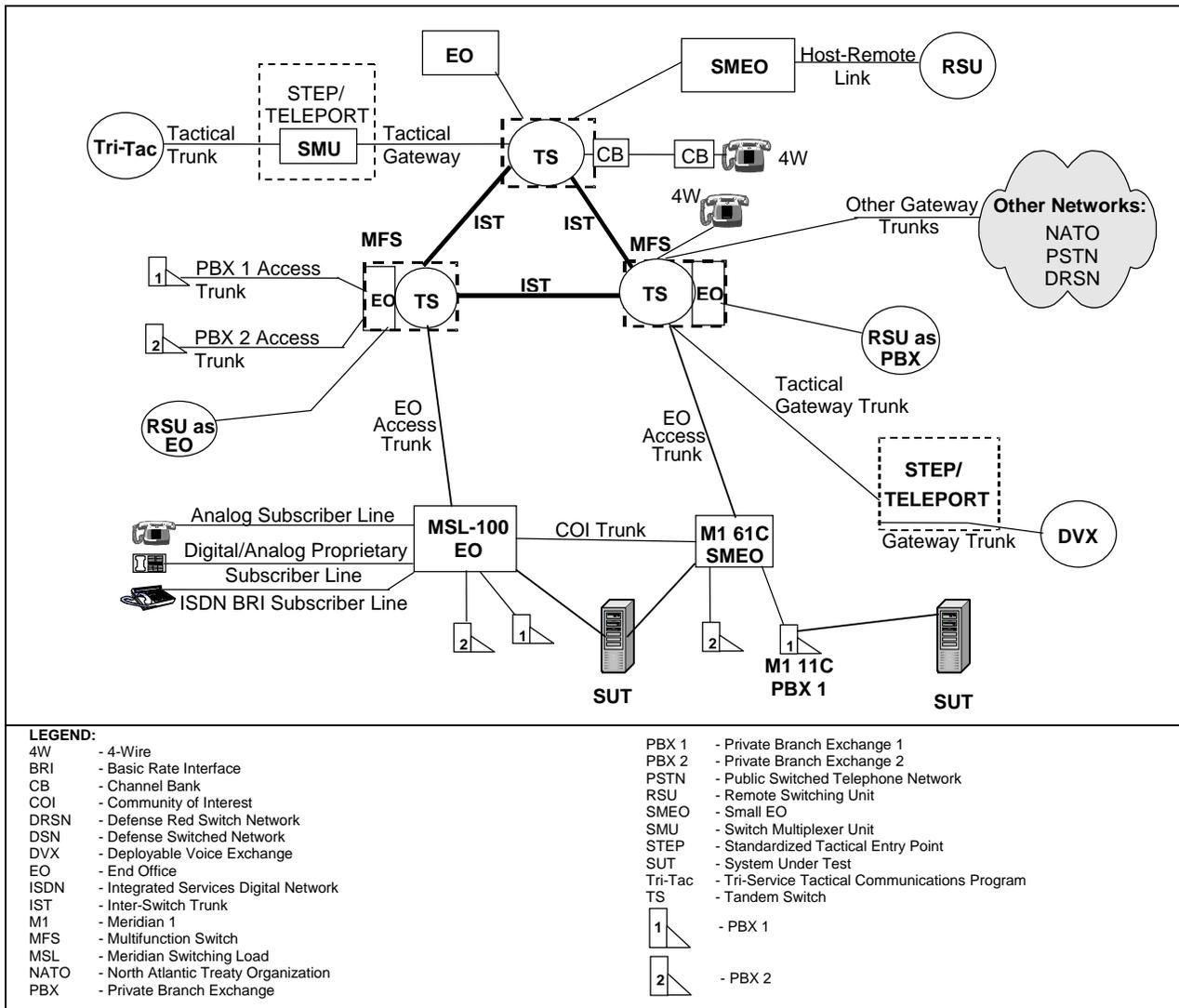


Figure 2-1. DSN Architecture

7. REQUIRED SYSTEM INTERFACES. Requirements specific to the SUT and interoperability results are listed in table 2-2. These requirements are derived from GSCR Interface and Functional Requirements (FRs) verified through JITC testing and/or vendor submission of Letter(s) of Compliance.

Table 2-2. SUT Functional Requirements and Interoperability Status

Interfaces	Critical	Certified	Functional Requirements	Met	GSCR Paragraph
Ethernet TCP/IP IEEE 802.3 (10BaseT)	No ¹	Yes	Fault Management (C)	Met	A.7.5
			Performance Management (C)	Met	
Ethernet TCP/IP IEEE 802.3.u (100BaseTX)	No ¹	Yes	Automated Message Accounting (C)	Met	
			Configuration Management (C)	Met	
EIA-232 Serial	No ¹	Yes	Security in accordance with DITSCAP (R)	Not Tested ²	A.7.6.5

LEGEND:
802.3 - IEEE standard for carrier sense multiple access with collision detection at 10 Mbps
802.3u - IEEE standard for carrier sense multiple access with collision detection at 100 Mbps
10BaseT - 10 Mbps (Baseband Operation, Twisted Pair) Ethernet
100BaseTX - 100 Mbps Ethernet over Category 5 Twisted Pair Copper
A - Appendix
C - Conditional
DISA - Defense Information Systems Agency
DITSCAP - Department of Defense Information Technology Security Certification and Accreditation Process
EIA - Electronic Industries Alliance
GSCR - Generic Switching Center Requirements
IEEE - Institute of Electrical and Electronics Engineers, Inc.
Mbps - Megabits per second
R - Required
SUT - System Under Test
TCP/IP - Transmission Control Protocol/Internet Protocol

NOTES:
¹ The Network Management requirements can be met via one of the following interfaces: Ethernet/TCP/IP (IEEE 802.3), Serial/Asynchronous (EIA-232), or Serial/Synchronous (X.25 and/or BX.25 variant)
² DITSCAP information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC's Global Information Grid Network Test Facility in a manner and configuration similar to that of the DSN operational environment. The test configuration depicted in figure 2-2 was used to test the system's interface functions and features.

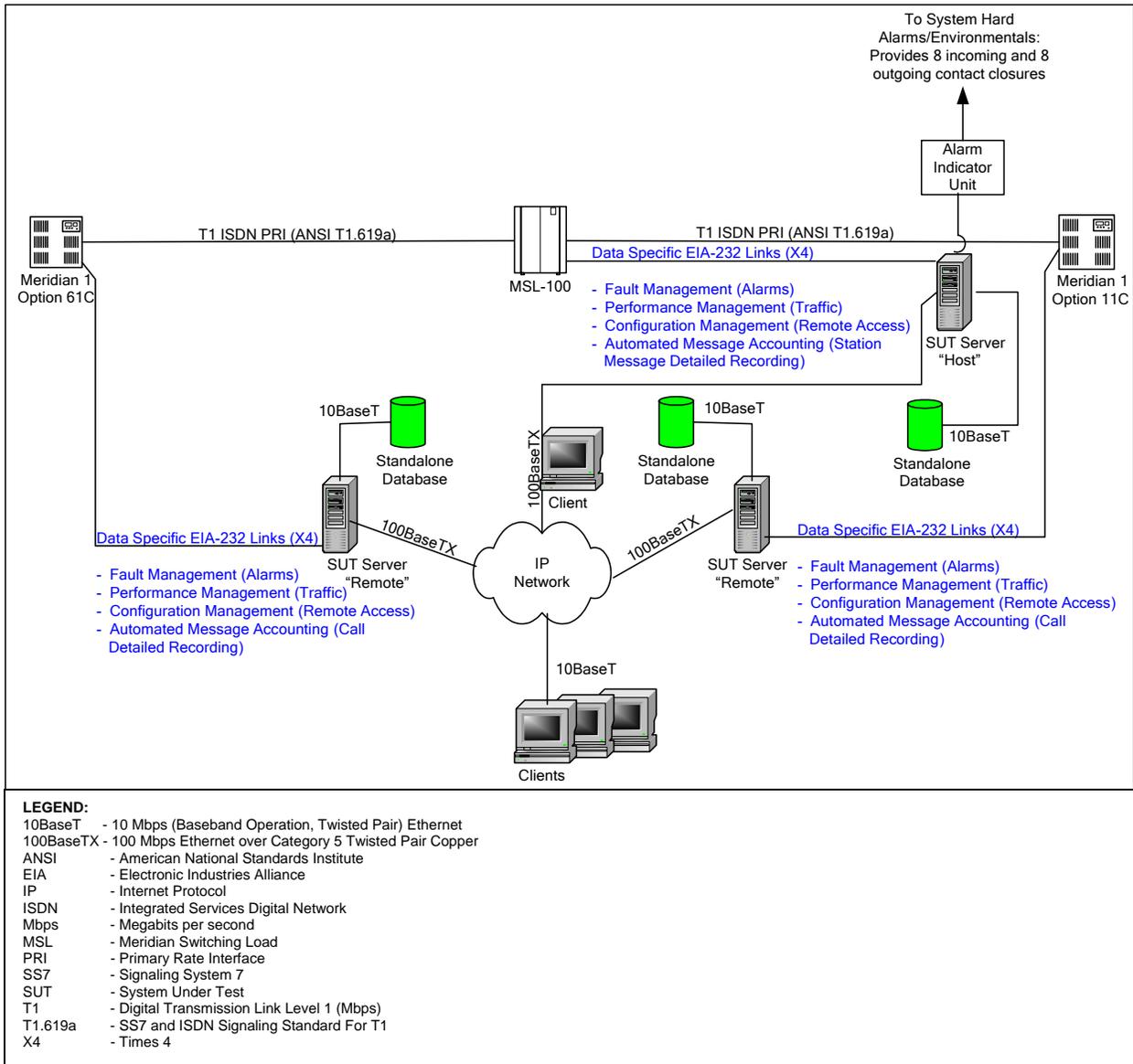


Figure 2-2. SUT Test Configuration

9. SYSTEM CONFIGURATIONS. The tested system configurations are shown in table 2-3.

- EIA-232 Link 2, 2400 baud: Operational Measurements, Automatic Call Distribution (ACD), Announcements, Conference Circuits, Office Traffic, Uniform Call Distribution, Attendant Consoles, Switch Performance Monitoring, Virtual Facility Groups, Hunt Groups, Remote Call Forwarding, Subscriber Line Usage, Line Modules, and Trunk Traffic. The SUT provides compiled traffic reports to ACD and console supervisors along with long-term traffic trending statistics essential for proper provisioning of trunk groups, lines, and modules.

- EIA-232 Link 3, 4800 baud: System Event Monitoring – Provides structured access to all log events generated by MSL-100, i.e., IBN110 Auth Abuse, LINE115 and LINE117 Calling Line Identification LINE125-136 Malicious Calls Trace.

- EIA-232 Link 4, 1200 baud: Command Line Polling – Provides a method of polling the secret log via logutil's OPENSURET commands. This process records all commands entered into the MSL-100 system by maintenance or service order personnel. This feature is also used to detect hackers attempting to access the MSL-100 system.

- EIA-232 Links 5-8 300-9600 baud: Secure Switch Access – Provides authorized clients command line access to the MSL-100 via video terminal emulation through the SUT server.

The SUT host collects all call detail records and system events from each provisioned remote. The SUT host also maintains the current alarm status of the network elements connected to each of its remotes.

2) SUT Remote Server. The SUT remote software is a fully functional server that performs all the tasks of data collection as the SUT host server. The only difference is its designation as a remote allowing it to send locally processed data to its host. The host/remote relationship allows maintenance and security personnel a single point of access to perform queries across the managed network elements. In the event of lost network connectivity between the host and remote, the SUT remote operates as a standalone server, which continues to process local switch data and respond to locally connected clients' requests.

3) SUT Client Access. The SUT Client access to the SUT servers is attained through:

- Transmission Control Protocol/Internet Protocol Port 80
- SUT server connections utilize AES 128 bit encryption

Detailed SUT and switch configurations can be found on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>.

c. Test Summary. The SUT met the critical interoperability requirements for a customer premise device for the interfaces shown in table 2-2, as set forth in reference (c), and is certified for joint use within the DSN.

12. TESTS 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), or <http://199.208.204.125> (SIPRNet). Information related to DSN testing is on the TSSI website at <http://jitc.fhu.disa.mil/tssi>.