



DEFENSE INFORMATION SYSTEMS AGENCY

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

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

24 Jan 13

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Fortinet, Incorporated FortiAnalyzer-2000B Release (Rel.) 4.3.6 and FortiManager-3000C Rel. 4.3.6

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for Interoperability (IO) test certification.
2. The FortiAnalyzer-2000B Rel. 4.3.6 and the FortiManager-3000C Rel. 4.3.6, hereinafter referred to as the Systems Under Test (SUTs), meet all critical IO requirements for Element Management Systems (EMS) and are certified for joint use within the Defense Information System Network (DISN). Both the FortiAnalyzer-2000B and the FortiManager-3000C perform similar network management functions for network devices (manage Fortinet data firewalls). The certification status of the SUT will be verified during operational deployment. Any new discrepancies noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of the Defense Information Systems Agency (DISA) via a vendor Plan of Actions and Milestones (POA&M) which addresses all new critical Test Discrepancy Reports (TDRs) within 120 days of identification. Testing was conducted using product requirements derived from the Unified Capabilities Requirements (UCR), Reference (c), and test procedures, Reference (d). No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that could affect IO, but no later than three years from the date of this memorandum.
3. This finding is based on IO testing conducted by the JITC, DISA adjudication of open TDRs, review of the vendor's Letters of Compliance (LoCs), and DISA Certification Authority (CA) approval of the IA configuration. The JITC, Indian Head, Maryland conducted IO testing from 1 through 8 February 2012. The DISA CA provided a positive Recommendation on 18 December 2012 based on the security testing completed by DISA Information Assurance (IA) test teams and published in a separate report, Reference (e).
4. Table 1 depicts the SUT Functional Requirements used to evaluate the interoperability of the SUT and the interoperability status.

Enclosure 1

Table 1. SUT Functional Requirements and Interoperability Status

Interface	Critical	Certified	Functional Requirements	Status	UCR Reference
IEEE 802.3u Ethernet	Yes	Yes	SNMPv3 format (R)	Met	5.3.2 See note 1.
			Alarm Messages (R)	Met	5.3.2.17.3.1.1
			Self-Detection of Fault Conditions (R)	Met	5.3.2.17.3.1.2
			SNMPv3 Format Alarm Messages (R)	Met	5.3.2.17.3.1.5
			Read-Write Access to CM Data by the VVoIP EMS (R)	Met	5.3.2.17.3.2.1
			Near-Real-Time Network Performance Monitoring (R)	Met	5.3.2.17.3.4.1
			Remote Network Management Commands (R)	Met	5.3.2.17.3.4.2
			Minimum Requirements (R)	Met	5.11.2
			Connectivity to Monitored Network Elements (R)	Met	5.11.2.1 See note 2.
			Segregation of NM Data into Categories (R)	Met	5.11.2.2
			IPv6 (C)	See note 3.	5.3.5
			DSCP Differentiated Service Code Point*	Met See note 4.	5.3.3.3.2
	Yes	Yes	Security (R)	See note 5.	Section 3

NOTES:

- Requirements as applied to the EMS.
- The SUT does not process CDRs; however, that requirement is not required.
- IPv6 is not supported by the SUT; however, the IPv6 support requirement has been deemed (CA/NS) not critical for EMS as long as the SUT does support IPv4. This requirement for EMS is optional.
- SUT does not support DSCP traffic tagging; however, as configured, the SUT does not pass management traffic past the internal management network. DSCP can be attained by completing suggested configuration requirements.
- Security is tested by DISA Information Assurance test teams and published in a separate report, Reference (e).

LEGEND:

802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	Mbps	Megabits per second
C	Conditional	NM	Network Management
CA	Certifying Authority	NS	Network Services
CDR	Call Detail Recording	R	Required
CM	Communication Manager	SNMPv3	Simple Network Management Protocol version 3
DISA	Defense Information Systems Agency	SUT	System Under Test
DSCP	Differentiated Services Code Point	TDR	Test Deficiency Report
EMS	Element Management System	UCR	Unified Capabilities Requirements
IEEE	Institute of Electrical and Electronics Engineers	VVoIP	Voice and Video over Internet Protocol
IPv4	Internet Protocol version 4		
IPv6	Internet Protocol version 6		

5. In accordance with the Program Manager’s request, JITC did not develop a detailed test report. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Non-secure Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program, which .mil/.gov users can access 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 at <http://jit.fhu.disa.mil> (NIPRNet). Information related to Approved Products List (APL) testing is available on the DISA APL Testing and Certification website located at <http://www.disa.mil/Services/Network-Services/UCCO>. All associated test information is available on the DISA Unified Capability Certification Office APL Integrated Tracking System (APLITS) website located at <https://aplits.disa.mil>.

JITC Memo, JTE, Interoperability Test Certification of the FortiAnalyzer-2000B Release (Rel.) 4.3.6 and FortiManager-3000C Rel. 4.3.6

6. The JITC point of contact is Mr. Kevin Holmes; commercial (301) 743-4300; e-mail address is Timothy.K.Holmes.civ@mail.mil. The JITC's mailing address is 3341 Strauss Ave., Ste. 236, Indian Head, MD 20640-5035. The tracking number for Fortinet, Inc. FortiAnalyzer-2000B Rel. 4.3.6 is 1122008 and FortiManager-3000C Rel. 4.3.6 is 1122010.

FOR THE COMMANDER:



for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

2 Enclosures a/s

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, MARCORSSYSCOM, SIAT, A&CE Division

US Coast Guard, CG-64

Defense Information Systems Agency, TEMC

DIA, Office of the Acquisition Executive

NSG Interoperability Assessment Team

DOT&E, Netcentric Systems and Naval Warfare

Medical Health Systems, JMIS IV&V

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, “Department of Defense Unified Capabilities Requirements 2008, Change 3,” September 2011
- (d) Joint Interoperability Test Command, “Unified Capabilities Test Plan (UCTP)”
- (e) Joint Interoperability Test Command, “Information Assurance (IA) Fortinet FortiAnalyzer2000B Rel. 4.3.6 DRAFT IA Assessment Report TN 1122008 and Fortinet FortiManager3000C Rel. 4.3.6 DRAFT IA Assessment Report TN 1122010”

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Fortinet, Incorporated FortiAnalyzer-2000B Release (Rel.) 4.3.6 and FortiManager-3000C Rel. 4.3.6, hereinafter referred to as the System Under Test (SUT).

2. SPONSOR. Mr. Michael Caruso, Marine Corps Network Operations and Security Center Enterprise Services, 27410 Hot Patch Road, Quantico, VA 22134, e-mail: michael.caruso@mcnosc.usmc.mil.

3. SYSTEM POC. Mr. Carl Erickson, 42616 St. Clair Lane, Leesburg, VA 20176, e-mail: cerickson@fortinet.com.

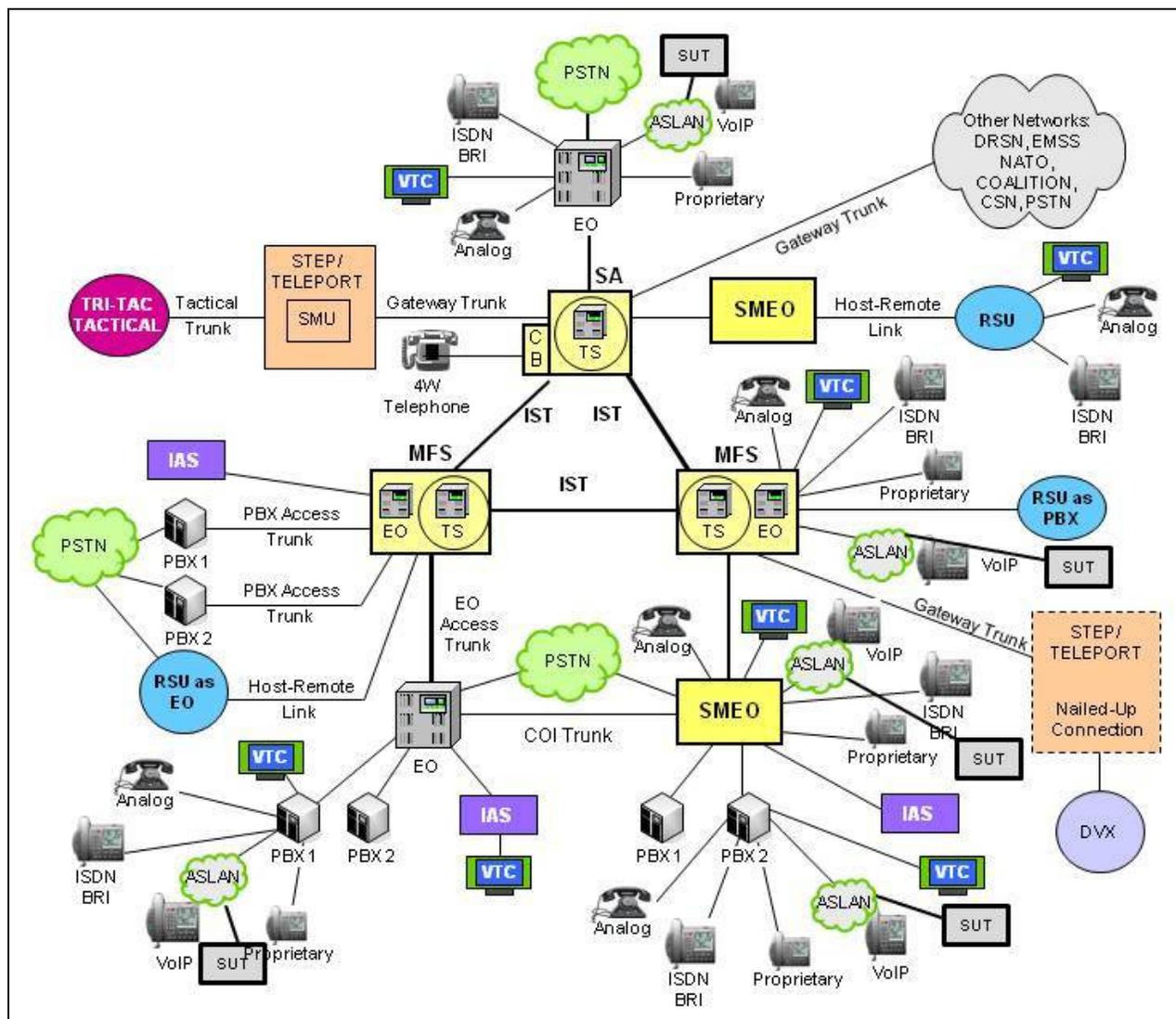
4. TESTER. Joint Interoperability Test Command (JITC), Indian Head, Maryland.

5. SYSTEM UNDER TEST DESCRIPTION. Defense Information Systems Agency has single system management responsibility for the Unified Capabilities (UC) Multifunction Soft-Switch, Edge Boundary Controllers and Local Session Controllers to include Legacy Defense Information System Network (DISN) Tandem Switches, Multifunction Switches, and End Office Switches. The SUT provides all Voice and Video over Internet Protocol (VVoIP) Element Management System (EMS) capabilities for the DISN including fault management, performance management, configuration management, accounting management, and remote access to switching platforms and key non-switch network elements.

Fortinet FortiManager-3000C. The FortiManager-3000C is an EMS that functions as a security management appliance. It provides centralized configuration management, policy-based provisioning, update management, and network monitoring for up to 5000 configured network devices. The FortiManager-3000C, when integrated with a FortiAnalyzer appliance, is part of a single point of command, control, analysis, and reporting for a network.

Fortinet FortiAnalyzer-2000B: The FortiAnalyzer-2000B security management appliance runs the FortiAnalyzer version 4.0 operating system (OS), which provides all operating functions, device configuration, and management access in a single integrated OS. In the test configuration, the FortiAnalyzer-2000B was functioning as a network traffic analysis device and network system log collector and archive device.

6. OPERATIONAL ARCHITECTURE. The Unified Capabilities Requirements (UCR) Legacy DSN architecture in Figure 2-1 and the UC notional architecture depicted in Figure 2-2 show the relationship of the SUT to the DSN and UC architectures.



LEGEND:

- | | | | |
|-------|-------------------------------------|---------|---|
| 4W | 4-Wire | PBX | Private Branch Exchange |
| ASLAN | Assured Services Local Area Network | PBX 1 | Private Branch Exchange 1 |
| BRI | Basic Rate Interface | PBX 2 | Private Branch Exchange 2 |
| COI | Community of Interest | PSTN | Public Switched Telephone Network |
| CSN | Canadian Switch Network | RSU | Remote Switching Unit |
| DRSN | Defense Red Switch Network | SA | Standalone |
| DSN | Defense Switched Network | SMEO | Small End Office |
| DVX | Deployable Voice Exchange | SMU | Switched Multiplex Unit |
| EMSS | Enhanced Mobile Satellite System | STEP | Standardized Tactical Entry Point |
| EO | End Office | SUT | System Under Test |
| IAS | Integrated Access Switch | TRI-TAC | Tri-Service Tactical Communications Program |
| ISDN | Integrated Services Digital Network | TS | Tandem Switch |
| IST | Interswitch Trunk | VoIP | Voice over Internet Protocol |
| MFS | Multi-Function Switch | VTC | Video Teleconferencing |
| NATO | North Atlantic Treaty Organization | | |

Figure 2-1. DSN Architecture

Table 2-1. SUT Functional Requirements and Interoperability Status

Interface	Critical	Certified	Functional Requirements	Status	UCR Reference
IEEE 802.3u Ethernet	Yes	Yes	SNMPv3 format (R)	Met	5.3.2 See note 1.
			Alarm Messages (R)	Met	5.3.2.17.3.1.1
			Self-Detection of Fault Conditions (R)	Met	5.3.2.17.3.1.2
			SNMPv3 Format Alarm Messages (R)	Met	5.3.2.17.3.1.5
			Read-Write Access to CM Data by the VVoIP EMS (R)	Met	5.3.2.17.3.2.1
			Near-Real-Time Network Performance Monitoring (R)	Met	5.3.2.17.3.4.1
			Remote Network Management Commands (R)	Met	5.3.2.17.3.4.2
			Minimum Requirements (R)	Met	5.11.2
			Connectivity to Monitored Network Elements (R)	Met	5.11.2.1 See note 2.
			Segregation of NM Data into Categories (R)	Met	5.11.2.2
			IPv6 (C)	See note 3.	5.3.5
DSCP Differentiated Service Code Point	Met See note 4.	5.3.3.3.2			
Yes	Yes	Security (R)	See note 5.	Section 3	

NOTES:

- Requirements as applied to the EMS.
- The SUT does not process CDRs; however it is not required to.
- IPv6 is not supported by the SUT; however, the IPv6 support requirement has been deemed (CA/NS) not critical for EMS as long as the device supports IPv4.
- SUT does not support DSCP traffic tagging; however, as configured, the SUT does not pass management traffic past the internal management network. DSCP can be attained by completing suggested configuration requirements.
- Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (e).

LEGEND:

802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	Mbps	Megabits per second
C	Conditional	NM	Network Management
CA	Certifying Authority	NS	Network Services
CDR	Call Detail Recording	R	Required
CM	Communication Manager	SNMPv3	Simple Network Management Protocol version 3
DISA	Defense Information Systems Agency	SUT	System Under Test
DSCP	Differentiated Services Code Point	TDR	Test Deficiency Report
EMS	Element Management System	UCR	Unified Capabilities Requirements
IEEE	Institute of Electrical and Electronics Engineers	VVoIP	Voice and Video over Internet Protocol
IPv4	Internet Protocol version 4		
IPv6	Internet Protocol version 6		

8. TEST NETWORK DESCRIPTION. The SUT was tested at the JITC's, Indian Head, Maryland Test Facility in a manner and configuration similar to that of the DISN operational environment. Testing the system's required functions and features was conducted using the test configurations depicted in Figure 2-2.

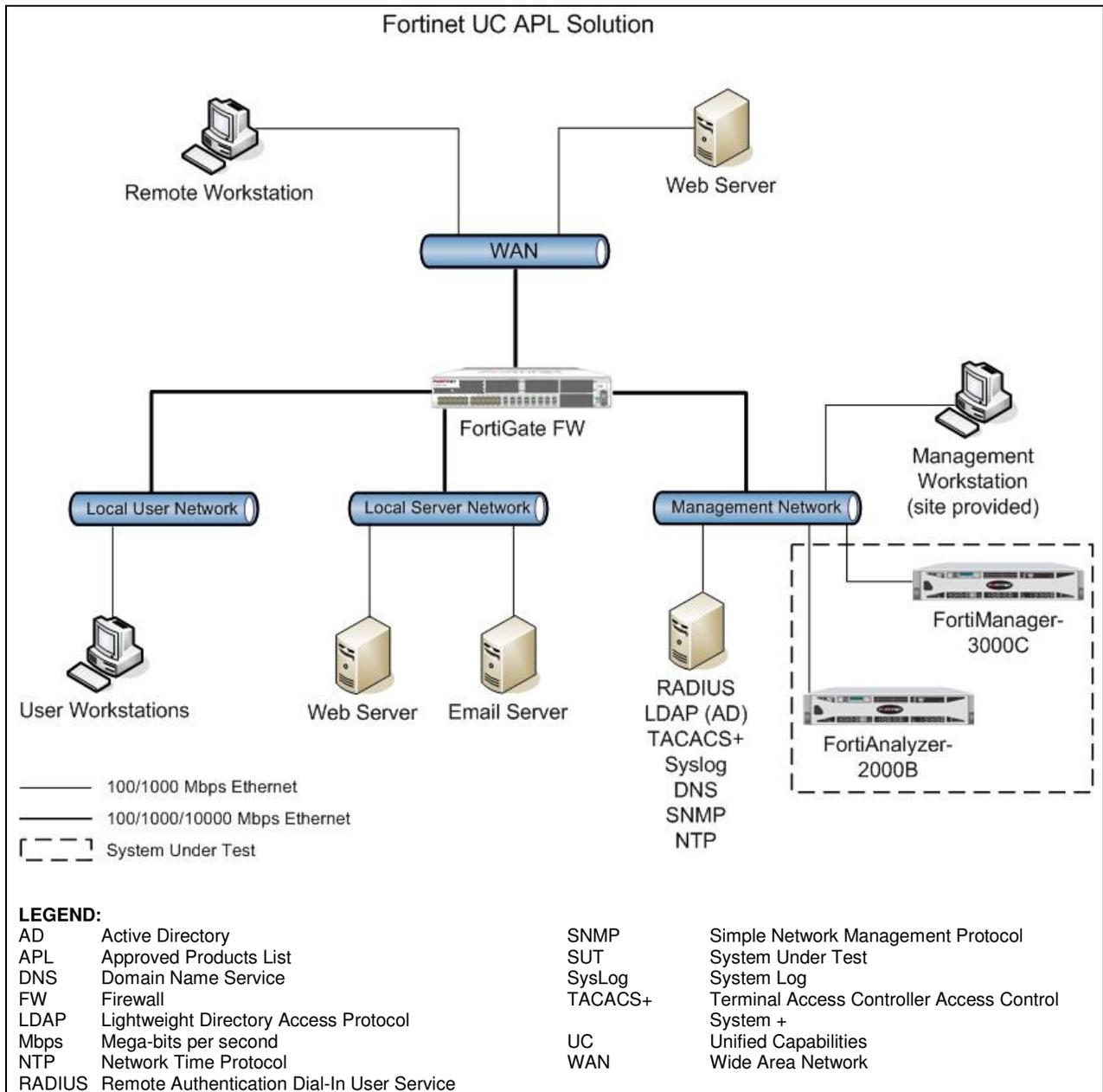


Figure 2-2. SUT Test Configuration

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 Cisco Assured Services Local Area Network (ASLAN) core layer components. The SUT is certified with any ASLAN core layer components that are on the UC Approved Product List (APL).

critical interoperability requirements for AMA by collecting and storing network traffic data.

(5) IAW the UCR 2008, Change 3, Sections 5.3.2 and 5.11, the UC switches must meet the switch performance data requirements in the UCR 2008, Change 3, Table 5.3.2.17-1. The SUT met all critical interoperability requirements for Performance Management by collecting and accurately storing traffic data measurements every five or fifteen minutes.

(6) The UCR 2008, Change 3, Sections 5.3.2 and 5.11, manual network management controls are those controls that are implemented by the personnel at a network management center. Manual controls supplement the automatic controls, and they are used to handle the network problems that require flexibility and human judgment. The SUT met all critical interoperability certification requirements for Features and Functions.

(7) IAW the UCR 2008, Change 3, Sections 5.3.2 and 5.11, the UC switching system shall be able to receive remote commands for configuring the network related entries within the switch. The SUT met all critical interoperability requirements for Remote Access by successfully connecting through the respective switching systems access channels.

(8) IAW UCR 2008, Change 3, paragraph 5.3.5, the product shall support the IPv6 networking protocol as specified for Network Appliances/Simple Servers. The SUT does not support Internet Protocol version 6 (IPv6); however, the IPv6 support requirement has been deemed by the Certifying Authority and Network Services as not critical for EMS devices as long as the device supports IPv4. This requirement was not met and a Test Deficiency Report will be filed.

(9) IAW UCR 2008, Change 3, paragraph 5.3.3.3.2, the product shall support the plain text Differentiated Services Code Point (DSCP) plan per UCR 2008, Change 3, Table 5.3.3-1, DSCP Assignments, and the DSCP assignment shall be software configurable for the full range (0-63) to support the Deployable deployments that may not use the DSCP plan in this table. The SUT does not support DSCP assignments; however, the SUT operates at an internal management network level where DSCP assignments are not required. DSCP assignments can be attained by completing suggested configuration requirements. The overall requirement is Not Applicable.

b. Test Summary. The SUT met the interface and functional requirements for VVoIP EMS as set forth in Reference (c).

12. TEST AND ANALYSIS REPORT. IAW the Program Manager's request, no detailed test report was developed. JITC distributes interoperability information via the JITC Electronic Report Distribution 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 at <http://jit.fhu.disa.mil> (NIPRNet). Information related to APL testing is available on the APL Testing and Certification website at <http://www.disa.mil/Services/Network-Services/UCCO>.