

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

IN REPLY
REFER TO:

Joint Interoperability Test Command (JITC)

18 Sept 12

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the Vocera Communication System with Software Release 4.1, Wireless End Instrument System

References: (a) Department of Defense Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) Department of Defense 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 test certification.

2. The Vocera Communication System with Software Release 4.1, is hereinafter referred to as the System Under Test (SUT). The SUT meets all its critical interoperability requirements and JITC certifies the SUT for joint use in the Defense Switch Network (DSN) as a Wireless End Instrument (WEI). The SUT connects to customer provided Private Branch Exchange system via its T1 Primary Rate Interface to provide voice-calling capabilities to the Vocera Mobile Communication Devices. The SUT does not support Military Unique Features (MUFs) and can only serve users having no requirement to originate Command and Control (C2) communications. Connectivity to DSN requires a waiver from the Chairman of the Joint Chiefs of Staff (CJCS) for each site. The operational status of the SUT must be verified during deployment. Any new discrepancies discovered in the operational environment will be evaluated for impact and adjudicated to the satisfaction of Defense Information Systems Agency (DISA) via a vendor Plan of Action and Milestones to address the concern(s) within 120 days of identification. JITC conducted testing using WEI requirements within the Unified Capabilities Requirements (UCR) 2008, Change 1, Reference (c), and other sponsor requested requirements. JITC tested the SUT using WEI test procedures, Reference (d) and test procedures developed to address sponsor unique requirements. JITC does not certify any other configurations, features, or functions, except those cited within this memorandum. This certification expires three years from placement on the Approved Products List (19 June 2015) or upon changes that affect interoperability.

3. These findings are based on interoperability testing conducted by JITC, review of the vendor's Letters of Compliance (LOC), and Information Assurance (IA) Certification Authority (CA) approval of the IA configuration. JITC conducted interoperability testing at the Indian Head, Maryland test facility from 8 through 25 May 2011. The DISA IA CA reviewed the JITC

JITC Memo, Special Interoperability Test Certification of the Vocera Communication System with Software Release 4.1, Wireless End Instrument (WEI) System

published IA Assessment Report for the SUT, Reference (e), and provided a positive recommendation of the IA configuration on 14 June 2012. The acquiring agency or site will be responsible for the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) accreditation. Enclosure 2 documents test results and describes the tested network and system configurations. Enclosure 3, System Functional and Capability Requirements, lists the WEI Capability Requirements (CR) and Functional Requirements (FR).

4. Section 5.3 of Reference (c) establishes threshold CRs/FRs used to evaluate interoperability of the SUT as a WEI. Tables 1 and 2 list the WEI interfaces, CRs, FRs, and the status of the requirements.

Table 1. SUT Interface Interoperability Status

Interface	Critical (See note 1)	UCR Reference (UCR 2008 CH 1)	Threshold CR/FR Requirements (See note 2)	Status	Remarks																												
Wireless Endless Instruments																																	
802.11a	No	5.3.1.7.2.3	1, 2, 3, and 4	N/A	Not supported																												
802.11b	No	5.3.1.7.2.3	1, 2, 3, and 4	Certified																													
802.11g	No	5.3.1.7.2.3	1, 2, 3, and 4	Certified																													
802.16	No	5.3.1.7.2.3	1, 2, 3, and 4	N/A	Not supported																												
Other																																	
T1 ISDN PRI	No	5.3.2.31.4.8	ANSI T1.607	Certified	See note 3.																												
<p>NOTES:</p> <p>1. The UCR does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).</p> <p>2. The SUT does not need to provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements. The detailed CR/FR requirements are listed in Enclosure 3.</p> <p>3. The Vocera Communications System provides wireless end instrument connectivity to a Base PBX via a T1 ISDN PRI interface. This interface is the commercial variant (ANSI T1.607) and does not provide MLPP C2 capabilities.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td>ANSI</td> <td>American National Standards Institute</td> <td>MLPP</td> <td>Multilevel Precedence and Preemption</td> </tr> <tr> <td>ASLAN</td> <td>Assured Services Local Area Network</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>C2</td> <td>Command and Control</td> <td>PBX</td> <td>Private Branch Exchange</td> </tr> <tr> <td>CH</td> <td>Change</td> <td>PRI</td> <td>Primary Rate Interface</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>UCR</td> <td>Unified capabilities Requirements</td> </tr> <tr> <td>ISDN</td> <td>Integrated Services Digital Network</td> <td></td> <td></td> </tr> </table>						ANSI	American National Standards Institute	MLPP	Multilevel Precedence and Preemption	ASLAN	Assured Services Local Area Network	N/A	Not Applicable	C2	Command and Control	PBX	Private Branch Exchange	CH	Change	PRI	Primary Rate Interface	CR	Capability Requirement	SUT	System Under Test	FR	Functional Requirement	UCR	Unified capabilities Requirements	ISDN	Integrated Services Digital Network		
ANSI	American National Standards Institute	MLPP	Multilevel Precedence and Preemption																														
ASLAN	Assured Services Local Area Network	N/A	Not Applicable																														
C2	Command and Control	PBX	Private Branch Exchange																														
CH	Change	PRI	Primary Rate Interface																														
CR	Capability Requirement	SUT	System Under Test																														
FR	Functional Requirement	UCR	Unified capabilities Requirements																														
ISDN	Integrated Services Digital Network																																

JITC Memo, Special Interoperability Test Certification of the Vocera Communication System with Software Release 4.1, Wireless End Instrument (WEI) System

Table 2. SUT CRs and FRs Status

CR/FR ID	Capability/ Function	Applicability (See note 1)	UCR Reference (UCR 2008 CH 1)	Status	Remarks																																																												
1	General Wireless Requirements																																																																
	IPv6	Required	5.3.1.7.2.1	Not Met	See note 2																																																												
	Wi-Fi Certified	Required	5.3.1.7.2.1	Not Met	See note 3																																																												
	F/FO	Required	5.3.1.7.2.1	Met																																																													
	Redundancy	Required	5.3.1.7.2.1	Met																																																													
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1	Met																																																													
	Latency	Required	5.3.1.7.2.1	Met																																																													
	Traffic Prioritization	Required	5.3.1.7.2.1	N/A																																																													
	Wireless STIGs	Required	5.3.1.7.2.1	Met																																																													
2	Wireless Interface Requirements																																																																
	Interface Standards	Required	5.3.1.7.2.3	Met																																																													
	802.11a Interface Standards	Required	5.3.1.7.2.3	N/A																																																													
	802.11b Interface Standards	Required	5.3.1.7.2.3	Met																																																													
	802.11g Interface Standards	Required	5.3.1.7.2.3	Met																																																													
	802.16 Interface Standards	Required	5.3.1.7.2.3	N/A																																																													
3	Wireless End Instruments																																																																
	VoIP Solution	Required	5.3.1.7.2.4	Met																																																													
	Access Methods	Required	5.3.1.7.2.4	Met																																																													
	Dedicated or Shared	Required	5.3.1.7.2.4	Met																																																													
	Call Control Authentication	Required	5.3.1.7.2.4	Met																																																													
	IP Telephone Switch	Required	5.3.1.7.2.4	Met																																																													
	FIPS 140-2 Level 1	Required	5.3.1.7.2.4	Met																																																													
	Call Termination	Required	5.3.1.7.2.4	Met																																																													
4	ASLAN Requirements Applicable to Wireless Products																																																																
	General Performance Parameters	Required	5.3.1.3	Met																																																													
<p>NOTES:</p> <p>1. The SUT need not provide wireless capability. However, if wireless capability is present, the wireless product shall support at least one of the following approved wireless LAN standards interfaces: 802.11a (WEI, WLAS, WAB), 802.11b (WEI, WLAS), 802.11g (WEI, WLAS, WAB), 802.16 (WEI, WLAS, WAB).</p> <p>2. Vendor's SUT was submitted under UCR 2008 Change 1, therefore IPV6 is not applicable. The IPV6 requirement for wireless was (and is under this submittal) conditional. DISA adjudicated SUT's lack of IPV6 compliance as "Minor" with Plans of Actions and Milestones for December 2012.</p> <p>3. Vendor's SUT is not Wi-Fi Alliance certified and was tested with a limited set of other Wi-Fi products. MILDEP accepts this risk in selected deployments.</p> <p>LEGEND:</p> <table border="0"> <tr> <td>802.11</td> <td>IEEE set of wireless standards in the 2.4,3.6, and 5 GHz frequency bands</td> <td>IP</td> <td>Internet Protocol</td> </tr> <tr> <td>802.16</td> <td>IEEE series of wireless broadband standards</td> <td>IPv6</td> <td>Internet Protocol version 6</td> </tr> <tr> <td>ASLAN</td> <td>Assured Services Local Area Network</td> <td>LAN</td> <td>Local Area Network</td> </tr> <tr> <td>BER</td> <td>Bit Error Rate</td> <td>MOS</td> <td>Mean Opinion Score</td> </tr> <tr> <td>CH</td> <td>Change</td> <td>MILDEP</td> <td>Military Departments</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>E2E</td> <td>End-to-end</td> <td>STIG</td> <td>Security Technical Implementation Guide</td> </tr> <tr> <td>EIs</td> <td>End Instruments</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>F/FO</td> <td>Flash/ Flash Override</td> <td>TDR</td> <td>Test Discrepancy Reports</td> </tr> <tr> <td>FIPS</td> <td>Federal Information Processing Standard</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>VoIP</td> <td>Voice over Internet Protocol</td> </tr> <tr> <td>GHz</td> <td>Gigahertz</td> <td>WAB</td> <td>Wireless Access Bridge</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>WEI</td> <td>Wireless End Instrument</td> </tr> <tr> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td>Wi-Fi</td> <td>Wireless Fidelity</td> </tr> <tr> <td></td> <td></td> <td>WLAS</td> <td>Wireless LAN Access System</td> </tr> </table>						802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz frequency bands	IP	Internet Protocol	802.16	IEEE series of wireless broadband standards	IPv6	Internet Protocol version 6	ASLAN	Assured Services Local Area Network	LAN	Local Area Network	BER	Bit Error Rate	MOS	Mean Opinion Score	CH	Change	MILDEP	Military Departments	CR	Capability Requirement	N/A	Not Applicable	E2E	End-to-end	STIG	Security Technical Implementation Guide	EIs	End Instruments	SUT	System Under Test	F/FO	Flash/ Flash Override	TDR	Test Discrepancy Reports	FIPS	Federal Information Processing Standard	UCR	Unified Capabilities Requirements	FR	Functional Requirement	VoIP	Voice over Internet Protocol	GHz	Gigahertz	WAB	Wireless Access Bridge	ID	Identification	WEI	Wireless End Instrument	IEEE	Institute of Electrical and Electronics Engineers	Wi-Fi	Wireless Fidelity			WLAS	Wireless LAN Access System
802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz frequency bands	IP	Internet Protocol																																																														
802.16	IEEE series of wireless broadband standards	IPv6	Internet Protocol version 6																																																														
ASLAN	Assured Services Local Area Network	LAN	Local Area Network																																																														
BER	Bit Error Rate	MOS	Mean Opinion Score																																																														
CH	Change	MILDEP	Military Departments																																																														
CR	Capability Requirement	N/A	Not Applicable																																																														
E2E	End-to-end	STIG	Security Technical Implementation Guide																																																														
EIs	End Instruments	SUT	System Under Test																																																														
F/FO	Flash/ Flash Override	TDR	Test Discrepancy Reports																																																														
FIPS	Federal Information Processing Standard	UCR	Unified Capabilities Requirements																																																														
FR	Functional Requirement	VoIP	Voice over Internet Protocol																																																														
GHz	Gigahertz	WAB	Wireless Access Bridge																																																														
ID	Identification	WEI	Wireless End Instrument																																																														
IEEE	Institute of Electrical and Electronics Engineers	Wi-Fi	Wireless Fidelity																																																														
		WLAS	Wireless LAN Access System																																																														

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

JITC Memo, Special Interoperability Test Certification of the Vocera Communication System with Software Release 4.1, Wireless End Instrument (WEI) System

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>.

6. The JITC point of contact is Ms. Jacquelyn Mastin, commercial 301-743-4320. Her e-mail address is Jacquelyn.mastin.civ@mail.mil, and mailing address 3341 Strauss Avenue, Suite 236, Indian Head, Maryland 20640-5149. The UCCO tracking number is 1016101.

FOR THE COMMANDER:

3 Enclosures a/s


for 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 MARCORSSYSCOM, 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

HQUSAISEC, AMSEL-IE-IS

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense Document, "Department of Defense Unified Capabilities Requirements 2008, Change 1," 22 January 2010
- (d) Joint Interoperability Test Command Document, "Unified Capabilities Test Plan (UCTP)," November 2009
- (e) Joint Interoperability Test Command, "Information Assurance (IA) Finding Summary for Vocera Communication System Release 4.1 (Tracking Number 1016101)," May 2011.

(This page intentionally left blank.)

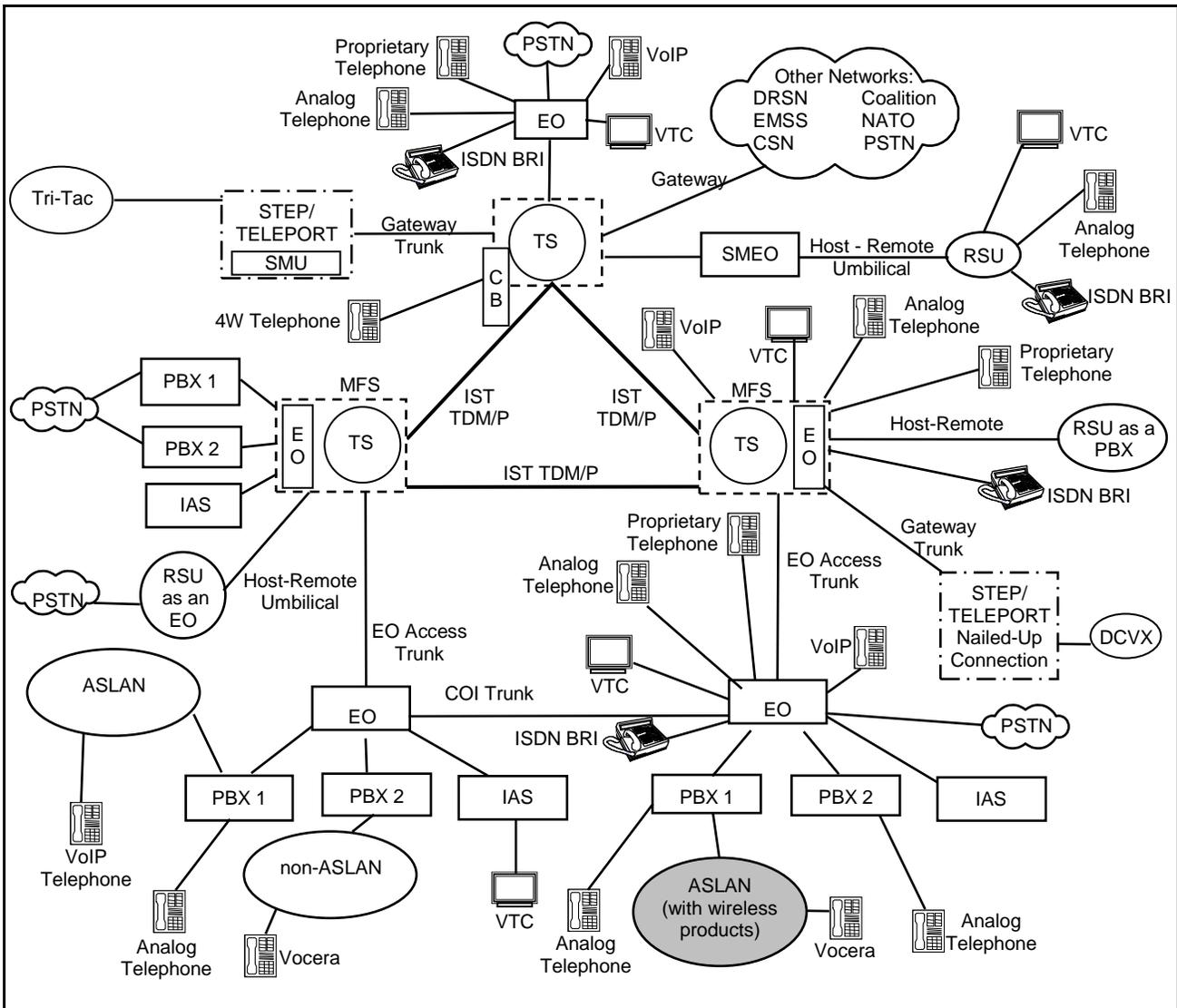
CERTIFICATION TESTING SUMMARY

- 1. SYSTEM TITLE.** The Vocera Communication System with Software Release 4.1, Wireless End Instrument (WEI) System.
- 2. SPONSOR.** Ms. Danielle Nicholson, Email: Danielle.A.Nicholson@us.army.mil.
- 3. SYSTEM POC.** Mr. David Maranick, Email: dmarancik@vocera.com
- 4. TESTER.** Joint Interoperability Test Command (JITC) Indian Head, Maryland
- 5. SYSTEM DESCRIPTION.** The Vocera Communication System (VCS), hereinafter referred to as the System Under Test (SUT), is a Commercial Off-the Shelf (COTS) product that enables users to communicate using Voice over IP (VOIP) through an existing wireless network infrastructure. The SUT provides users with voice calling capability through Vocera Mobile Communication Devices, which leverage the existing wireless network.

A customer provided Private Branch Exchange (PBX) Telephony system provides voice-calling capabilities to Vocera Mobile Communication Devices. The Vocera Telephony Interface Server has a hardware link connection using an Intel(r) Dialogic(r) Board to connect to an analog T1, T1 relay, or Integrated Services Digital Network (ISDN) connection to a PBX switch on an existing telephony infrastructure. Additionally, the VCS provides metric reporting including system usage, logs and activity, access and performance. The system is comprised of four components: the Vocera Communication Server, the Vocera Telephony Interface Server, the Vocera Reports Server and the Vocera Mobile Communication Badge. Vocera deploys server software and badge hardware. Vocera does not supply server hardware or third party telephony components.

The Vocera Communication Server routes calls, and sessions between the Vocera Communications Badges and the other components of the Vocera Communication System, as well as provides the Vocera Mobile Communication Badges with voice command recognition. The Vocera Telephony Interface server allows the Vocera Mobile Communication Badges to place and receive calls from the existing telephony infrastructure. Finally, the Vocera Reports Server allows creation of reports on analysis of the data gathered by the Vocera Communication Server, including device and user access information, system usage, performance, device status and other customizable options.

- 6. OPERATIONAL ARCHITECTURE.** JITC tested the SUT under WEI Unified Capabilities Requirements (UCR) product category. A high-level Defense Switched Network (DSN) node architecture is depicted in Figure 2-1 and displays the relationship of the SUT to the DSN switches.



LEGEND:

- | | | | |
|-------|-------------------------------------|---------|---|
| 4W | 4-Wire | NATO | North Atlantic Treaty Organization |
| ASLAN | Assured Services Local Area Network | PBX | Private Branch Exchange |
| BRI | Basic Rate Interface | PBX 1 | Private Branch Exchange 1 |
| CB | Channel Bank | PBX 2 | Private Branch Exchange 2 |
| COI | Community of Interest | PSTN | Public Switched Telephone Network |
| CSN | Canadian Switch Network | RSU | Remote Switching Unit |
| DCVX | Deployable Cellular Voice Exchange | SMEO | Small End Office |
| DRSN | Defense Red Switch Network | SMU | Switched Multiplex Unit |
| DSN | Defense Switched Network | STEP | Standardized Tactical Entry Point |
| EMSS | Enhanced Mobile Satellite System | SUT | System Under Test |
| EO | End Office | TDM/P | Time Division Multiplexing/Packetized |
| IAS | Integrated Access Switch | Tri-Tac | Tri-Service Tactical Communications Program |
| ISDN | Integrated Services Digital Network | TS | Tandem Switch |
| IST | Inter-switch Trunk | VoIP | Voice over Internet Protocol |
| MFS | Multifunction Switch | VTC | Video Teleconferencing |

Figure 2-1. DSN Architecture

7. INTEROPERABILITY REQUIREMENTS. The interface, Capability Requirements (CR), Functional Requirements (FR), Information Assurance (IA), and other requirements for wireless products are established by Section 5.3.1 of the Department of Defense (DoD) UCR 2008, Change 1, Reference (c).

7.1 Interfaces. The wireless products use its interfaces to connect to the Assured Services Local Area Network (ASLAN) infrastructure and wireless devices (voice, video, and data). The threshold requirements for interfaces specific to the wireless products are listed in Table 2-1.

Table 2-1. Wireless Interface Requirements

Interface	Critical (See note 1)	UCR Reference (UCR 2008 CH 1)	Threshold CR/FR Requirements (See note 2)	Status	Remarks
Wireless Endless Instruments					
802.11a	No	5.3.1.7.2.3	1, 2, 3, and 4	Meet minimum CR/FRs and 802.11 interface standards.	
802.11b	No	5.3.1.7.2.3	1, 2, 3, and 4		
802.11g	No	5.3.1.7.2.3	1, 2, 3, and 4		
802.16	No	5.3.1.7.2.3	1, 2, 3, and 4		
Other					
T1 ISDN PRI	No	5.3.2.31.4.8	ANSI T1.607	Meet minimum CR/FRs	See note 3
NOTES:					
1. The UCR does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).					
2. The SUT does not need to provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements. The detailed CR/FR requirements are listed in Enclosure 3.					
3. The Vocera Communications System provides wireless end instrument connectivity to a Base PBX via a T1 ISDN PRI interface. This interface is the commercial variant (ANSI T1.607) and does not provide MLPP C2 capabilities.					
LEGEND:					
ANSI	American National Standards Institute	ISDN	Integrated Services Digital Network		
ASLAN	Assured Services Local Area Network	MLPP	Multilevel Precedence and Preemption		
C2	Command and Control	PBX	Private Branch Exchange		
CH	Change	PRI	Primary Rate Interface		
CR	Capability Requirement	UCR	Unified capabilities Requirements		
FR	Functional Requirement				

7.2 CR and FR. Wireless products have required and conditional features and capabilities established by Section 5.3.1.7.2 of the UCR. The SUT is not required to provide non-critical (conditional) features and capabilities. If they are provided, they must function according to the specified requirements. Table 2-2 lists the features and capabilities and their associated requirements for SUT products. Table 3-1 of Enclosure 3 provides detailed CR/FR requirements.

Table 2-2. Wireless Capability Requirements and Functional Requirements

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH 1)	Criteria	Remarks
General Wireless Requirements					
1	IPv6	Required	5.3.1.7.2.1	Meet minimum UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WLAN product types
	Wi-Fi Certified	Required	5.3.1.7.2.1		
	F/FO	Required	5.3.1.7.2.1		
	Redundancy	Required	5.3.1.7.2.1		
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1		
	Latency	Required	5.3.1.7.2.1		
	Traffic Prioritization	Required	5.3.1.7.2.1		
	Wireless STIGs	Required	5.3.1.7.2.1		
Wireless Intrusion Detection System					
2	Continuous Scanning	Required	5.3.1.7.2.2	See Table 3-1 of Enclosure 3.	Applies to WLAS and WAB product types
	Location-sensing	Required	5.3.1.7.2.2		
Wireless Interface Requirements					
3	Interface Standards	Required	5.3.1.7.2.3	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WEI, WLAS, and WAB product types
	802.11a Interface Standards	Required	5.3.1.7.2.3		
	802.11b Interface Standards	Required	5.3.1.7.2.3		
	802.11g Interface Standards	Required	5.3.1.7.2.3		
	802.16 Interface Standards	Required	5.3.1.7.2.3		
Wireless End Instruments					
4	VoIP Solution	Required	5.3.1.7.2.4	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WEI product types
	Access Methods	Required	5.3.1.7.2.4		
	Dedicated or Shared	Required	5.3.1.7.2.4		
	Call Control Authentication	Required	5.3.1.7.2.4		
	IP Telephone Switch	Required	5.3.1.7.2.4		
	FIPS 140-2 Level 1	Required	5.3.1.7.2.4		
	Call Termination	Required	5.3.1.7.2.4		
Wireless LAN Access System					
5	Loss of Call upon WLAS failure	Required	5.3.1.7.2.5	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WLAS only.
	Maximum supported EIs	Required	5.3.1.7.2.5		
	MOS	Required	5.3.1.7.2.5		
	Roaming	Required	5.3.1.7.2.5		
Wireless Access Bridge					
6	802.16 Interface Standards	Required	5.3.1.7.2.6	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WAB only.
	Maximum Voice Calls Transported	Required	5.3.1.7.2.6		
	Voice MOS	Required	5.3.1.7.2.6		
	E2E BER	Required	5.3.1.7.2.6		
	Secure Voice Transmission	Required	5.3.1.7.2.6		
	Call Signaling Transport	Required	5.3.1.7.2.6		
	Latency	Required	5.3.1.7.2.6		
	Jitter	Required	5.3.1.7.2.6		
	WLAS/WAB Combination	Required	5.3.1.7.2.6		

**Table 2-2. Wireless Capability Requirements and Functional Requirements
(continued)**

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH 1)	Criteria	Remarks																																																																																				
7	ASLAN Requirements Applicable to Wireless Products																																																																																								
	General Performance Parameters	Required	5.3.1.3	See Table 3-1 of Enclosure 3.																																																																																					
<p>NOTE: The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.</p> <p>LEGEND:</p> <table border="0"> <tr> <td>802.11</td> <td>IEEE set of wireless standards in the 2.4,3.6, and 5 GHz</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>802.16</td> <td>IEEE series of wireless broadband standards</td> <td></td> <td>IP</td> <td>Internet Protocol</td> <td></td> </tr> <tr> <td>ASLAN</td> <td>Assured Services Local Area Network</td> <td></td> <td>IPv6</td> <td>Internet Protocol version 6</td> <td></td> </tr> <tr> <td>BER</td> <td>Bit Error Rate</td> <td></td> <td>LAN</td> <td>Local Area Network</td> <td></td> </tr> <tr> <td>CH</td> <td>Change</td> <td></td> <td>MOS</td> <td>Mean Opinion Score</td> <td></td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td></td> <td>STIG</td> <td>Security Technical Implementation Guide</td> <td></td> </tr> <tr> <td>E2E</td> <td>End-to-end</td> <td></td> <td>SUT</td> <td>System Under Test</td> <td></td> </tr> <tr> <td>EIs</td> <td>End Instruments</td> <td></td> <td>UCR</td> <td>Unified Capabilities Requirements</td> <td></td> </tr> <tr> <td>F/FO</td> <td>Flash/Flash Override</td> <td></td> <td>VoIP</td> <td>Voice over Internet Protocol</td> <td></td> </tr> <tr> <td>FIPS</td> <td>Federal Information Processing Standard</td> <td></td> <td>WAB</td> <td>Wireless Access Bridge</td> <td></td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td></td> <td>WEI</td> <td>Wireless End Instrument</td> <td></td> </tr> <tr> <td>GHz</td> <td>Gigahertz</td> <td></td> <td>Wi-Fi</td> <td>Wireless Fidelity</td> <td></td> </tr> <tr> <td>ID</td> <td>Identification</td> <td></td> <td>WLAS</td> <td>Wireless LAN Access System</td> <td></td> </tr> <tr> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td></td> <td>WLAN</td> <td>Wireless Local Area Network</td> <td></td> </tr> </table>						802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz					802.16	IEEE series of wireless broadband standards		IP	Internet Protocol		ASLAN	Assured Services Local Area Network		IPv6	Internet Protocol version 6		BER	Bit Error Rate		LAN	Local Area Network		CH	Change		MOS	Mean Opinion Score		CR	Capability Requirement		STIG	Security Technical Implementation Guide		E2E	End-to-end		SUT	System Under Test		EIs	End Instruments		UCR	Unified Capabilities Requirements		F/FO	Flash/Flash Override		VoIP	Voice over Internet Protocol		FIPS	Federal Information Processing Standard		WAB	Wireless Access Bridge		FR	Functional Requirement		WEI	Wireless End Instrument		GHz	Gigahertz		Wi-Fi	Wireless Fidelity		ID	Identification		WLAS	Wireless LAN Access System		IEEE	Institute of Electrical and Electronics Engineers		WLAN	Wireless Local Area Network	
802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz																																																																																								
802.16	IEEE series of wireless broadband standards		IP	Internet Protocol																																																																																					
ASLAN	Assured Services Local Area Network		IPv6	Internet Protocol version 6																																																																																					
BER	Bit Error Rate		LAN	Local Area Network																																																																																					
CH	Change		MOS	Mean Opinion Score																																																																																					
CR	Capability Requirement		STIG	Security Technical Implementation Guide																																																																																					
E2E	End-to-end		SUT	System Under Test																																																																																					
EIs	End Instruments		UCR	Unified Capabilities Requirements																																																																																					
F/FO	Flash/Flash Override		VoIP	Voice over Internet Protocol																																																																																					
FIPS	Federal Information Processing Standard		WAB	Wireless Access Bridge																																																																																					
FR	Functional Requirement		WEI	Wireless End Instrument																																																																																					
GHz	Gigahertz		Wi-Fi	Wireless Fidelity																																																																																					
ID	Identification		WLAS	Wireless LAN Access System																																																																																					
IEEE	Institute of Electrical and Electronics Engineers		WLAN	Wireless Local Area Network																																																																																					

7.3 Other. The SUT requires connectivity to an existing PBX in order to provide voice communications and signaling. The VCS connects to a base PBX via a commercial T1 ISDN PRI.

Table 2-3. Other Interface Requirements

Interface	Critical	UCR Reference (UCR 2008 CH 1)	Criteria	Remarks																
T1 ISDN PRI	No	5.3.2.31.4.8	ANSI T1.607	See note.																
<p>NOTE: The Vocera Communications System provides wireless end instrument connectivity to a Base PBX via a T1 ISDN PRI interface. This interface is the commercial variant (ANSI T1.607) and does not provide MLPP C2 capabilities.</p> <p>LEGEND:</p> <table border="0"> <tr> <td>ANSI</td> <td>American National Standards Institute</td> <td>MLPP</td> <td>Multilevel Precedence and Preemption</td> </tr> <tr> <td>C2</td> <td>Command and Control</td> <td>PBX</td> <td>Private Branch Exchange</td> </tr> <tr> <td>CH</td> <td>Change</td> <td>PRI</td> <td>Primary Rate Interface</td> </tr> <tr> <td>ISDN</td> <td>Integrated Services Digital Network</td> <td>UCR</td> <td>Unified capabilities Requirements</td> </tr> </table>					ANSI	American National Standards Institute	MLPP	Multilevel Precedence and Preemption	C2	Command and Control	PBX	Private Branch Exchange	CH	Change	PRI	Primary Rate Interface	ISDN	Integrated Services Digital Network	UCR	Unified capabilities Requirements
ANSI	American National Standards Institute	MLPP	Multilevel Precedence and Preemption																	
C2	Command and Control	PBX	Private Branch Exchange																	
CH	Change	PRI	Primary Rate Interface																	
ISDN	Integrated Services Digital Network	UCR	Unified capabilities Requirements																	

8. TEST NETWORK DESCRIPTION. JITC tested the SUT at its Indian Head, Maryland Wireless Test laboratory, from 8 through 25 May 2011. Figures 2.2 and 2-3 shows the SUT's test configuration.

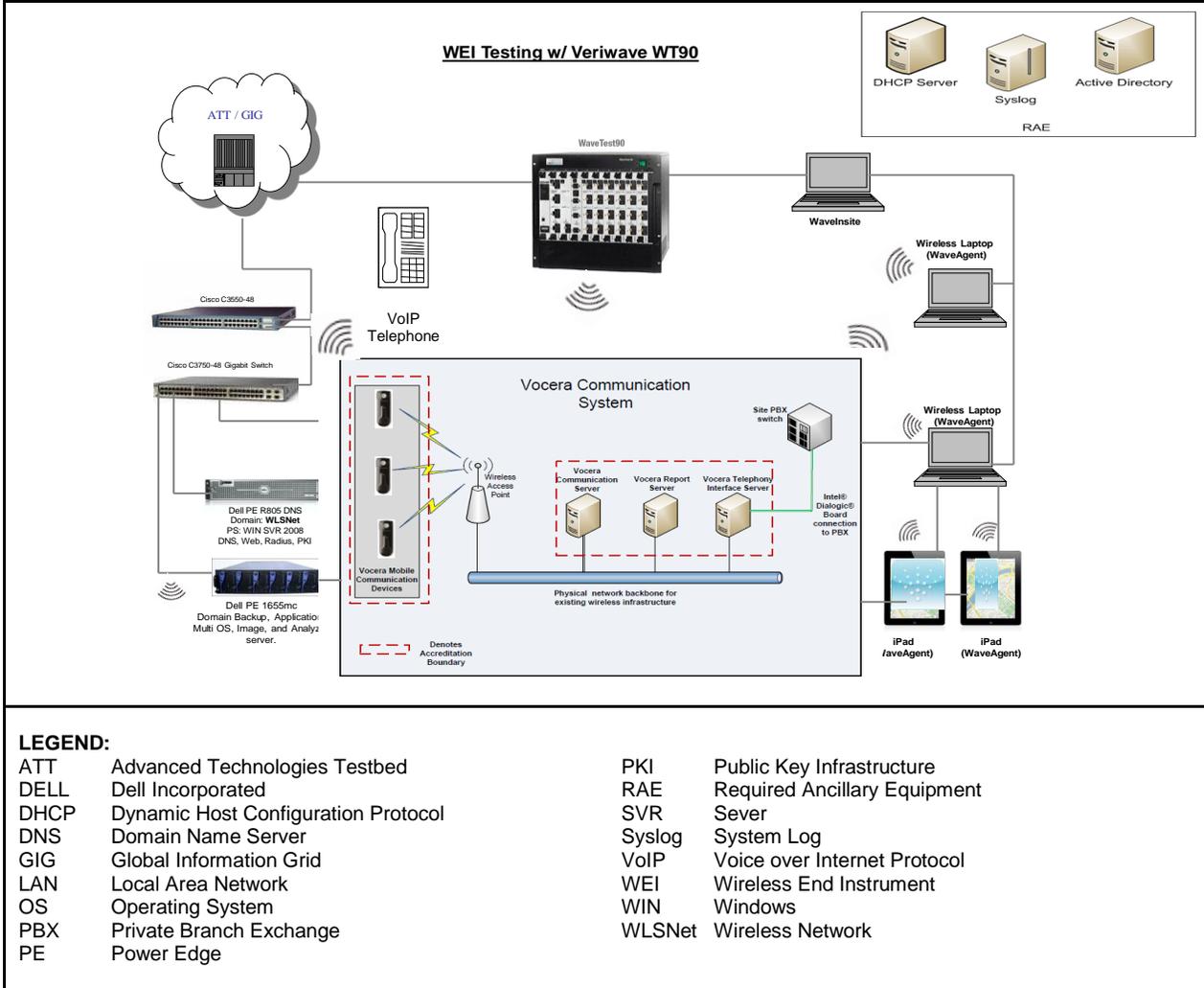


Figure 2-2. WEI B2000 Test Configuration 1

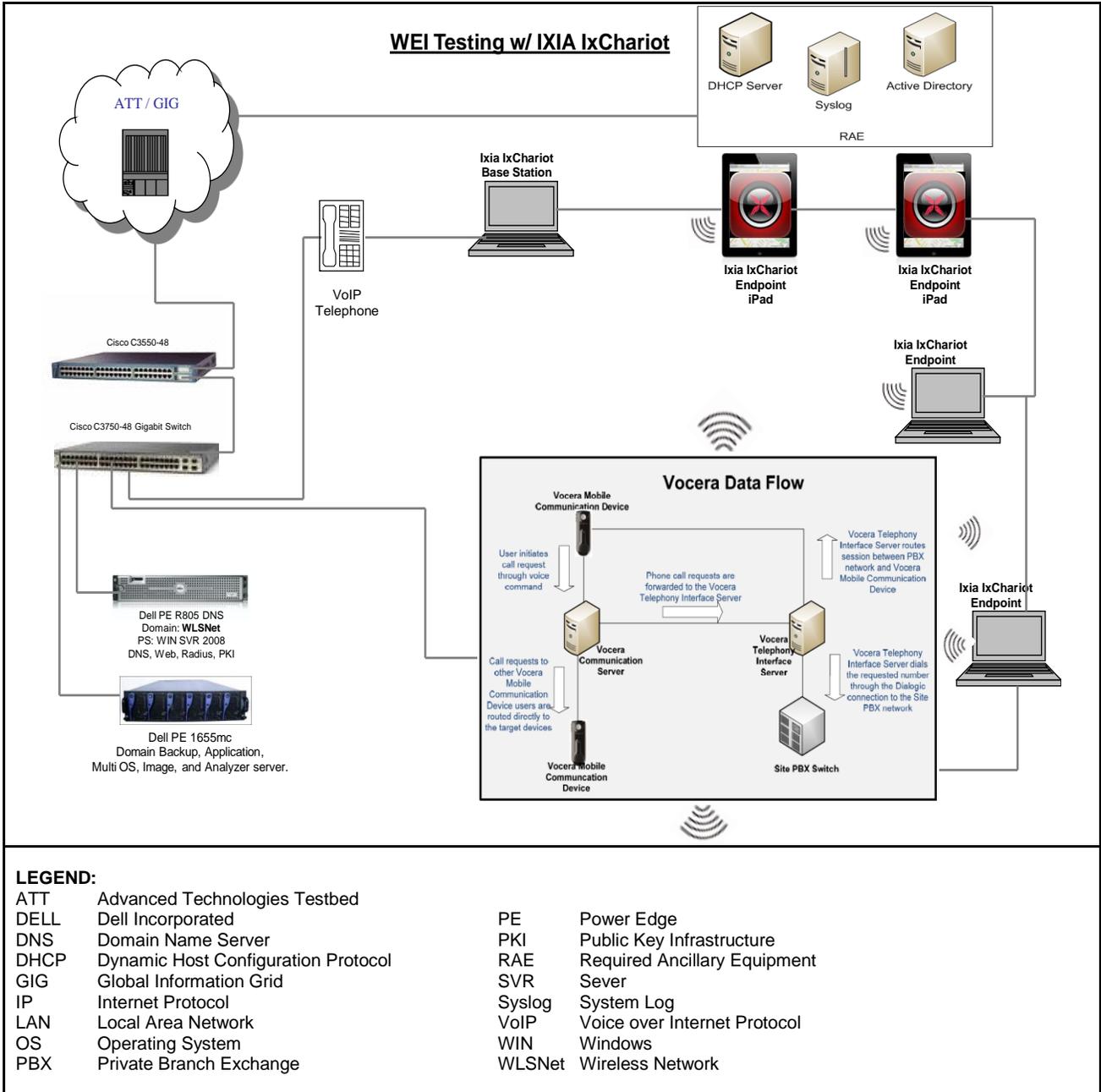


Figure 2-3 WEI B2000 Test Configuration 2

9. SYSTEM CONFIGURATIONS. Table 2-3 lists tested SUT equipment shown in Figure 2-2, Table 2-4 lists Non-SUT equipment used to test the SUT, and Table 2-5 lists test tools used during the assessment.

Table 2-4. System Equipment

System Name	Software/Firmware	Versions	Hardware	Qty
Vocera Communication Server	Vocera System Software	4.1	Dell Precision T3400 Customer Provided	1
	Nuance	8.5.0		
	MYSQL Database	5.0.84		
	Sun Java JRE	1.5.0_10		
	Apache Tomcat	4.1.39		
	Apache HTTP Server	2.0.63		
	Windows Server 2003	SP2		
Vocera Telephony Interface Server	Dialogic Drivers and Configuration	SP2	IBM e Server Series 206 Customer Provided	1
	Windows 2003 Server			
Vocera Reports Server	Eclipse	3.1	Dell Dimension 4300 Customer Provided	1
	MYSQL Database	5.0.84		
	Apache Tomcat	4.1.39		
	Java Runtime Environment	1.5.0_10		
	Business Objects	11 r2		
	Windows Server 2003	SP2		
Vocera Mobile Communication Device/Badge	Embedded Linux Kernel	2.6.16-R3-omap1	Vocera Mobile Communication Device Customer Provided	10
LEGEND:				
HTTP	Hypertext Transfer Protocol	omap	platform software	
IBM	International Business Machines	R	Release	
JRE	Java Runtime Environment	SP	Service pack	
MYSQL	My Structured Query Language			

Table 2-5. Non-SUT Equipment

Component	Software Version	Function/Capability	
Redcom PBX	V6.1a	Provide and allow voice-calling capabilities to the Vocera Mobile Communication Devices/badges.	
Cisco Aironet Access Points	AP1242AG-A-KG*	Wireless Access Point	
Cisco IP Phones	CP-7911	Accept and send calls to the Vocera communication badge.	
Management Workstation	Windows XP SP3	Provides Management/Administration Console of the Vocera System. It is a browser-based application, accessible from any computer on the same dedicated VLAN.	
Active Directory	Windows Server 2003 SP2	Authenticates and authorizes users and Vocera servers on the VLAN.	
GFE CAC/PKI Workstation	ActivIdentity ActivClient 6.2.0.133	Facilitating use of PKI authentication and establishing authoritative process for use of identity credentials.	
DHCP Server	V.1.2	Assign IP addresses dynamically to the Vocera Badges.	
LEGEND:			
a	part of the version	PBX	Private Branch Exchange
APs	Access Points	PKI	Public Key Infrastructure
CAC	Common Access Card	SP	Service pack
CP	Cisco Phone	SysLog	System Log
DHCP	Dynamic Host Configuration Protocol	V	Version
GFE	Government Furnished Equipment	VLAN	Virtual Local Area Network
IP	Internet Protocol	WLAN	Wireless Local Area Network
PBX	Private Branch Exchange		

Table 2-6. Test Tools / Equipment

Manufacture	Type	Port Type	Software Version
Veriwave	Traffic generator / capture SUT's behavior and performance from the exact point of view of the end-user.	AP port	V 2.0
IXia	Packet Generator	AX/4000 MAX IP PoS/ATM/FR OC-12c/OC-3c/STM-OC-12c/OC-3c/STM-	V 4.81.0
WireShark	Packet Analyzer	TCP/UDP	V.1.4.13
Flying Squirrel	Wireless Discovery/Mapping Application	TCP/UDP	V.1.4.0
LEGEND: ATM Asynchronous Transfer Mode AP Access Point IP Internet Protocol MAX Maximum OC Optical Carrier PoS Packet Over Synchronous Optical Network STM Synchronous Transport Module SUT System Under Test TCP Transmission Control Protocol UDP User Datagram Protocol V Version			

10. TESTING LIMITATIONS.

a. The Cisco Aironet Access Point (AP) was the sole AP device used by JITC during the testing of VCS to validate wireless connectivity.

b. The Redcom PBX was the sole PBX device used by JITC during testing of VCS to validate the capability of the Intel(r) Dialogic(r) Board hardware interface that enable call dialing and receiving capabilities in the test lab.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for WEI and JITC certifies its use within the DSN. Additional discussion regarding specific testing results is located in subsequent paragraphs.

11.1 Interfaces. The SUT's wireless interface status is provided in Table 2-7.

Table 2-7. SUT Interface Requirements Status

Interface	Critical (See note 1)	UCR Reference (UCR 2008 CH 1)	Threshold CR/FR Requirements (See note 2)	Status	Remarks
Wireless Endless Instruments					
802.11a	No	5.3.1.7.2.3	1, 2, 3, and 4	N/A	Not supported
802.11b	No	5.3.1.7.2.3	1, 2, 3, and 4	Certified	
802.11g	No	5.3.1.7.2.3	1, 2, 3, and 4	Certified	
802.16	No	5.3.1.7.2.3	1, 2, 3, and 4	N/A	Not supported
Other					
T1 ISDN PRI	No	5.3.2.31.4.8	ANSI T1.607	Certified	See note 3.
NOTES:					
1. The UCR does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).					
2. The SUT does not need to provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements. The detailed CR/FR requirements are listed in Enclosure 3.					
3. The Vocera Communications System provides wireless end instrument connectivity to a Base PBX via a T1 ISDN PRI interface. This interface is the commercial variant (ANSI T1.607) and does not provide MLPP C2 capabilities.					
LEGEND:					
ANSI	American National Standards Institute		MLPP	Multilevel Precedence and Preemption	
ASLAN	Assured Services Local Area Network		N/A	Not Applicable	
C2	Command and Control		PBX	Private Branch Exchange	
CH	Change		PRI	Primary Rate Interface	
CR	Capability Requirement		SUT	System Under Test	
FR	Functional Requirement		UCR	Unified capabilities Requirements	
ISDN	Integrated Services Digital Network				

11.2 Capability Requirements and Functional Requirements. The SUT's CR and FR status are provided in Table 2-8. Detailed CR/FR requirements are provided in Enclosure 3, Table 3-1.

Table 2-8. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/ Function	Applicability (See note 1)	UCR Reference (UCR 2008 CH 1)	Status	Remarks
General Wireless Requirements					
1	IPv6	Required	5.3.1.7.2.1	Not Met	See note 2
	Wi-Fi Certified	Required	5.3.1.7.2.1	Not Met	See note 3
	F/FO	Required	5.3.1.7.2.1	Met	
	Redundancy	Required	5.3.1.7.2.1	Met	
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1	Met	
	Latency	Required	5.3.1.7.2.1	Met	
	Traffic Prioritization	Required	5.3.1.7.2.1	N/A	
	Wireless STIGs	Required	5.3.1.7.2.1	Met	
Wireless Interface Requirements					
2	Interface Standards	Required	5.3.1.7.2.3	Met	
	802.11a Interface Standards	Required	5.3.1.7.2.3	N/A	
	802.11b Interface Standards	Required	5.3.1.7.2.3	Met	
	802.11g Interface Standards	Required	5.3.1.7.2.3	Met	
	802.16 Interface Standards	Required	5.3.1.7.2.3	N/A	
Wireless End Instruments					
3	VoIP Solution	Required	5.3.1.7.2.4	Met	
	Access Methods	Required	5.3.1.7.2.4	Met	
	Dedicated or Shared	Required	5.3.1.7.2.4	Met	
	Call Control Authentication	Required	5.3.1.7.2.4	Met	
	IP Telephone Switch	Required	5.3.1.7.2.4	Met	
	FIPS 140-2 Level 1	Required	5.3.1.7.2.4	Met	
	Call Termination	Required	5.3.1.7.2.4	Met	

Table 2-8. SUT Capability Requirements and Functional Requirements Status (continued)

4	ASLAN Requirements Applicable to Wireless Products				
	General Performance Parameters	Required	5.3.1.3	Met	
NOTES:					
1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.					
2. Vendor's SUT was submitted under UCR 2008 Change 1, therefore IPV6 is not applicable. The IPV6 requirement for wireless was (and is under this submittal) conditional. DISA adjudicated SUT's lack of IPV6 compliance as "Minor" with Plans of Actions and Milestones for December 2012.					
3. Vendor's SUT is not Wi-Fi Alliance certified and was tested with a limited set of other Wi-Fi products. MILDEP accepts this risk in selected deployments.					
LEGEND:					
802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz	IEEE	Institute of Electrical and Electronics Engineers		
802.16	IEEE series of wireless broadband standards	IP	Internet Protocol		
ASLAN	Assured Services Local Area Network	IPv6	Internet Protocol version 6		
BER	Bit Error Rate	MOS	Mean Opinion Score		
CH	Change	N/A	Not Applicable		
CR	Capability Requirement	QoS	Quality of Service		
E2E	End-to-end	STIG	Security Technical Implementation Guide		
EIs	End Instruments	SUT	System Under Test		
F/FO	Flash/ Flash Override	UCR	Unified Capabilities Requirements		
FIPS	Federal Information Processing Standard	VoIP	Voice over Internet Protocol		
FR	Functional Requirement	WAB	Wireless Access Bridge		
GHz	Gigahertz	WEI	Wireless End Instrument		
ID	Identification	Wi-Fi	Wireless Fidelity,		
		WLAS	Wireless LAN Access System		

a. General Wireless Requirements

(1) Internet Protocol version 6 (IPv6). If an IP interface is provided in any of the wireless components, then it shall meet the IP requirements detailed in the DoD Profile for IPv6 in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.1(1). The product was submitted 11 Feb 2010 while UCR 2008 change 1 was the governing requirements. The IPv6 req. for wireless was (and is under this submittal) conditional. Hence accept vendor offer of Minor with Plans of Actions and Milestones- December 2012; per Dr. Sweeney recommendation.

(2) Wi-Fi Certified. All 802.11 wireless products must be Wi-Fi Alliance Certified and shall be certified at the Enterprise level for Wi-Fi (Trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies including WLAN) Protected Access Level 2 (WPA2) in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.1(2). The SUT is not Wi-Fi Alliance Certified and was tested with a limited set of other Wi-Fi products. MILDEP accepts this risk in selected deployments.

(3) Flash/Flash Override (F/FO) Users. Wireless networks may support Priority/Routine, non-mission critical users, and Immediate but shall not be used to support F/FO users in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.1(3). JITC verified this requirement through the Call Control Agent database and Network Architecture that the SUT is not configured to support Flash/Flash Override subscribers and only routine subscribers are authorized.

(4) Redundancy. For wireless products that provide transport to more than 96 mission critical telephony users, the wireless products shall provide redundancy and WLAS and/or associated WLAN controller/ switches that provide and/or control voice services to more than 96 WEIs shall provide redundancy through either single or dual product redundancy in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.1(4). JITC used SUT WEI test configurations to confirm this requirement. Tester confirmed that all components support redundancy by initiating a test system failure. The SUT uses a redundant combination of active and standby nodes, called cluster. The cluster provided a high availability when the following events occurred: computer hardware, Vocera server, Nuance service, Vocera telephony Server and My Structured Query Language (MySQL) service failed.

No Voice over Internet Protocol (VoIP) call dropped that was directly attributed to the SUT. The association of the lower level operating system monitoring of the Internet Control Message Protocol (ICMP) Pings supports the test assessment of successful redundancy support for the SUT.

(5) FIPS 140-2 SUT is Level 1 certified. All wireless connections shall be Federal Information Processing Standard (FIPS) 140-2 Level 1 certified (connections may either be WEI to WLAS if both support FIPS 140-2 Level 1, or WEI to a FIPS 140-2 compliant product through a WLAS if the WLAS is not capable of FIPS 140-2 Level 1). Wireless products that comprise the WLAN shall be secured in accordance with their wireless security profile as FIPS 140-2 Level 1 or FIPS 140-2 Level 2 in accordance with UCR 2008 Change 1, Section 5.3.1.7.2.1(5). JITC verified that the SUT met the requirements through vendor submitted Letter of Compliance (LoC).

(6) Latency. The use of wireless in the LAN shall not increase latency by more than 10 milliseconds (ms) above the specified maximum latency for a wired LAN in accordance with UCR 2008 Change 1, Section 5.3.1.7.2.1 (6). JITC Indian Head, Maryland established a management session to the SUT WEI under test configurations to confirm this requirement. JITC measured latency for the SUT WEI at less than three milliseconds (ms) using WireShark to record VOIP Latency. Latency is the amount of time that it takes for a frame to be transported through the System Under Test (SUT). Since this time can vary, the latency measurement is made by sampling the transport time of many individual frames. Latency is an important performance metric as it determines how the SUT will handle forwarding traffic that is sensitive to delay. Any real-time protocol such as Voice is sensitive to latency.

(7) Traffic Prioritization. The WLAN shall support LAN Traffic Prioritization and Quality of Service (QoS) in accordance with the wireless interface type in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.1 (7). JITC verified the SUT does not provide Traffic Prioritization as this requirement is applicable to WLAN. Therefore, the requirement is not applicable.

(8) Wireless STIG. Wireless products shall meet the WLAN security requirements as stipulated in the Wireless Security Technical Implementation Guide

(STIG) and specified requirements of UCR 2008 Change 1 Section 5.3.1.7.2.1 (8). JITC verified that the SUT meets Wireless STIG requirements with mitigations, as detailed in IA Findings Report for this UC submission.

b. Wireless Interface Requirements

(1) Interface Standards. If a wireless product is used, the wireless product shall support at least one of the following approved wireless LAN standards interfaces in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.3 (1):

- 802.11a (WEI, WLAS, WAB)
- 802.11b (WEI ,WEI)
- 802.11g (WEI, WEI)
- 802.16 (WEI, WLAS, WAB)

JITC used the SUT WEI test configuration to confirm this requirement. The SUT has current WPA2 Certifications on file addressing the IEEE 802.11 b/g. This was also collaborated in the SUT vendor's LoC. Testers confirmed successful wireless associations and SUT interoperability with two different vendor wireless client interfaces. Tests were conducted successfully in each of the IEEE 802.11 b/g modes. The SUT does not support IEEE 802.11a or 802.16 interfaces.

(2) 802.11 Interface Standards. For any of the 802.11 interfaces, the wireless product must support the following two 802.11 standards: 802.11e-Part 11 Amendment 8 and 802.11i-Part 11 Amendment 6 in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.3(2).

Tests were conducted successfully in each of the IEEE 802.11 b/g modes.

(3) 802.11a Interface Standards. For the 802.11a interface, the wireless product must support the standard 802.11h - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.3(3). JITC verified that the SUT does not support 802.11a interfaces through documentation and test configurations using Flying Squirrel.

(4) 802.16 Interface Standards. For any of the 802.16 interfaces, the wireless product must support the following 802.16 standards dependent on whether the end item attached to the WLAS is "fixed" or "nomadic" in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.3(4). JITC verified the SUT does not provide the conditionally required 802.16 interface. Fixed / Nomadic WEIs. JITC verified the SUT does not include the conditionally required WEIs.

c. WEI Requirements. JITC verified the SUT does provide a WEI solution, so

all WEI requirements are applicable.

(1) VoIP Solution. Wireless VoIP End Instruments (EIs) is certified as part of the VoIP solution in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.4 (1). JITC validated and verified the SUT is certified as part of the VoIP Solution through various configurations, system design documentation, performance, integration and system testing using Flying Squirrel, VeriWave and Ixia tools.

(2) Access Methods. Use 802.11 or 802.16 Access to/from a WEI shall be provided by either 802.11 or 802.16. Two methods that an IP subscriber can use to access voice services are dedicated wireless service or shared wireless service. The dedicated access method provides wireless access service for a single type of traffic (i.e., voice, video, or data – three devices are required to support all traffic types). The shared access method allows a single wireless WLAS to provide for all traffic types supported (i.e., voice, video, and data – one device provides all three traffic types), on all computer types and/or Personal Equipment Product (PED) to connect to the wireless WLAS in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.4(2). JITC verified that the SUT met the requirements through the use of test cases, validation tools such as Flying Squirrel and test configuration that the SUT uses the 802.11 standard to access voice services.

(3) Dedicated or Shared Access Method. WEIs may use either method separately or a combination to provide wireless access in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.4(3). JITC verified that the SUT met the requirements through test configurations for Dedicated Access Method with the use of a segregated VLAN.

(4) Call Control Authentication. WEIs or soft clients on workstations acting as WEIs shall authenticate to the VoIP system call control. Authentication shall be IAW UCR IA-specified requirements in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.4(4). JITC verified that the SUT met the requirements through validating user authentication and the use of Voice Print Recognition by carrying out various performance testing within test cases.

(5) IP Telephone Switch. The WEI is associated with the supporting IP telephone switch. The WEI shall be functionally identical to a traditional IP wired telephone and will be required to provide voice features and functionality IAW other UCR specified requirements unless explicitly stated in accordance with UCR 2008 Change 1 Section 5.3.1.7.2.4(5). JITC verified that the SUT met the requirements through test configurations and was able to provide voice functionality with an IP telephone.

(6) FIPS 140-2 Level 1. Minimally, all WEIs shall be FIPS 140-2 Level 1 certified. JITC verified the SUT met the requirements through vendor submitted LoC.

(7) Call Termination. If the WEI loses connection with the VoIP switch when using a WLAN, the call will be terminated by the VoIP switch. The termination period shall be determined by the VoIP switch using a configurable time-out parameter with a time-out range of 0-60 seconds; default shall be set to 5 seconds. The subscriber line will be treated as if it were out of service until communication is re-established with the wireless voice end instrument. JITC verified that the SUT met the requirements through test configurations and the SUT timeout within ten seconds after losing connectivity to the WLAN.

d. ASLAN Requirements Applicable to Wireless Products. The wireless products must meet the general performance parameters applicable for access devices in accordance with UCR 2008 Change 1 Section 5.3.1.3. JITC verified the SUT met the appropriate requirements as detailed in the previous paragraphs for the wireless interfaces. The JITC verified connectivity and UCR requirements for the wired interlaces. The SUT met the requirements for 10/100/1000 Mbps wired interfaces.

11.3 Information Assurance. The IA Assessment Report is published as a separate report, Reference (e).

11.4 Other. None.

12. TEST AND ANALYSIS REPORT. 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>.

(This page intentionally left blank.)

SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

Wireless products have required and conditional features established by the Unified Capabilities Requirements (UCR). The System Under Test (SUT) need not provide conditional features and capabilities; however, if they are present, they must function according to the specified requirements. The detailed Functional Requirements (FR) and Capability Requirements (CR) for wireless products are listed in Table 3-1. These requirements were taken from UCR Change 1 and all acronym definitions can be found in that document.

Table 3-1. Wireless Products Capability/Functional Requirements

ID	Requirement	UCR Reference (URC 2008 CH 1)	WLANS	WAB	WLAS	WEI
1	Meet the IP requirements detailed in the DISA UCR 2008 IPv6 Requirements.	UCR 2008: 5.3.1.7.2.1 (1)	R			
2	802.11 wireless products must be Wi-Fi alliance certified and shall be certified at the enterprise level for WPA2.	UCR 2008: 5.3.1.7.2.1 (2)	R			
3	Wireless networks may support I/P, R, and non-mission critical users, but shall not be used to support F/FO users.	UCR 2008: 5.3.1.7.2.1 (3)	R			
4	<p>For wireless products that provide transport to more than 96 mission critical telephony users, the wireless products shall provide redundancy and WLAS and/or associated WLAN controller/ switches that provide and/or control voice services to more than 96 WEIs shall provide redundancy through either:</p> <p>a. Single Product Redundancy. Shall have the following as a minimum: Dual power supplies/processors /radio systems/Ethernet ports; redundancy protocol; and no single point of failure for more than 96 subscribers.</p> <p>b. Dual product redundancy. Shall be collocated or co-adjacent and shall have the following as a minimum: traffic engineering to support all users on a single product upon failure of the other product. Secondary product may be on full standby or traffic sharing, supporting 50 percent of the traffic before failure rollover.</p>	UCR 2008: 5.3.1.7.2.1 (4)	R			
5	<p>All wireless connections shall be Federal Information Processing Standard (FIPS) 140-2 Level 1 certified (connections may either be WEI to WLAS if both support FIPS 140-2 Level 1, or WEI to a FIPS 140-2 compliant product through a WLAS if the WLAS is not <i>DoD UCR 2008, Change 1</i> Section 5.3.1 – ASLAN Infrastructure 127 capable of FIPS 140-2 Level 1). Wireless products that comprise the WLAN shall be secured in accordance with their wireless security profile as follows:</p> <p>a. FIPS 140-2, Level 1. Wireless components must be operated from within a “limited access, secure room” and be under user positive control at all times. However, if the wireless end item is designed to be left</p>	UCR 2008: 5.3.1.7.2.1 (5)	R			

Table 3-1. Wireless Products Capability/Functional Requirements (Continued)

ID	Requirement	UCR Reference (URC 2008 CH 1)	WLANS	WAB	WLAS	WEI
	<p>unattended, such as a wireless free-standing desk telephone, then that wireless end item must be Level 2 compliant.</p> <p>b. FIPS 140-2, level 2. Wireless components can be operated in an open public area such as an "open hallway," but recommend the use of a "limited access, secure room" if available and/or operationally feasible</p>					
6	<p>The use of wireless in the LAN shall not increase latency by more than 10 MS above the specified maximum latency for a wired LAN.</p>	UCR 2008: 5.3.1.7.2.1 (6)	R			
7	<p>The WLAN shall support LAN Traffic Prioritization and QoS IAW the following based on the wireless interface type:</p> <p>a. 802.11 Interfaces. Wireless products using 802.11 shall use the settable Service Class tagging/QoS parameters within 802.11e to implement, as a minimum, DSCP.</p> <p>b. 802.16 Interfaces. Wireless products using 802.16d and/or 802.16e, QoS/Service Class tagging shall meet the following requirements:</p> <p>(1) The WLAN products may use 802.16 services to provide QoS over the wireless portion of the transport. Services associated with the granular service class are listed in Table 5.3.1-7, Cable Grade Capabilities.</p> <p>(2) The WLAS and WABs shall mark traffic traversing into the wired portion of the LAN with appropriate wired DSCPS (see table 5.3.1-7, 802.16 service scheduling).</p>	UCR 2008: 5.3.1.7.2.1 (7)	R			
8	<p>Wireless products shall meet the WLAN security requirements as stipulated in the Wireless Security Technical Implementation Guide (STIG) and the following specified requirements:</p> <p>All 802.11 wireless components shall:</p> <p>(1) Use the Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP). It will be implemented in 802.11i system encryption modules.</p> <p>(2) Implement the extensible authentication protocol - transport layer security (EAP-TLS) mutual authentication for the EAP component of Wi-Fi protected access (WPA2). This requirement does not apply to connections between 802.11 WABs.</p>	UCR 2008: 5.3.1.7.2.1 (8)	R			
9	<p>Continuous scanning: The WIDS will scan continuously around-the-clock to detect authorized and unauthorized activity.</p>	UCR 2008 5.3.1.7.2.2 (1)		R	R	
10	<p>Location-sensing WIDS: The WIDS will include a location sensing protection scheme for authorized and unauthorized wireless products.</p>	UCR 2008 5.3.1.7.2.2 (2)		R	R	
11	<p>Deployed systems shall be properly</p>	UCR 2008 5.3.1.7.2.2 (2)		R	R	

Table 3-1. Wireless Products Capability/Functional Requirements (Continued)

ID	Requirement	UCR Reference (URC 2008 CH 1)	WLANS	WAB	WLAS	WEI
	engineered so that the WLAN and wireless products achieve the required performance requirements in their specific structural environment. Users shall submit their network design with their request for DSN connection. The Unified Capabilities Connection Office (UCCO) submittal shall include wireless security compliancy FIPS 140 and proposed accessibility as well as WIDS National Information Assurance Partnership (NIAP) Common Criteria validation for basic robustness. Medium robustness will be applied, as determined by the Designated Approving Authority (DAA), when the NIAP Common Criteria for that level is approved.					
12	If a wireless product is used, the wireless product shall support at least one of the following approved wireless LAN standards interfaces: a. 802.11a (WEI, WLAS, WAB) b. 802.11b (WEI, WLAS) c. 802.11g (WEI, WLAS, WAB) d. 802.16 (WEI, WLAS, WAB).	UCR 2008: 5.3.1.7.2.3 (1)		R	R	R
13	For any of the 802.11 interfaces, the wireless product must support the following two 802.11 standards: a. 802.11e - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. See Table 5.3.1-6, Cable Grade Capabilities, for priority bit assignment. b. 802.11i - part 11: wireless LAN Medium Access Control (MAC) and physical layer specifications and amendment 6: MAC security enhancements.	UCR 2008: 5.3.1.7.2.3 (2)		R	R	R
14	For the 802.11a interface, the wireless product must support the standard 802.11h - part 11: wireless LAN MAC and physical layer (phy) specifications, amendment 5: spectrum and transmit power management extensions in the 5 GHz band in Europe.	UCR 2008: 5.3.1.7.2.3 (3)		R	R	R

Table 3-1. Wireless Products Capability/Functional Requirements (Continued)

ID	Requirement	UCR Reference (URC 2008 CH 1)	WLANS	WAB	WLAS	WEI
15	<p>For any of the 802.16 interfaces, the wireless product must support the following 802.16 standards dependent on whether the end item attached to the WLAS is "fixed" or "nomadic."</p> <p>a. Fixed WEIs are those WEIs that access a single WLAS during the session and are not expected to traverse between WLASs so that handoffs are not required. Fixed WEIs may support either 802.16d – Part 16: Air Interface for Fixed Broadband Wireless Access Systems or 802.16e – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, & Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1.</p> <p>b. Nomadic WEIs are those WEIs that are mobile and may traverse different WLAS during a single session. Nomadic WEIs must support 802.16e – part 16: air interface for fixed and mobile broadband wireless access systems, and amendment 2: physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1.</p>	UCR 2008: 5.3.1.7.2.3 (4)		R	R	R
16	Wireless VoIP EIS are certified as part of the VoIP solution.	UCR 2008: 5.3.1.7.2.4 (1)				R
17	Access to/from a WEI shall be provided by either 802.11 or 802.16. Two methods that an IP subscriber can use to access voice services are dedicated wireless service or shared wireless service (see figure 5.3.1-8, access methods for the wireless access layer end item product telephones). The dedicated access method provides wireless access service for a single type of traffic (i.e., voice, video, or	UCR 2008: 5.3.1.7.2.4 (2)				R

Table 3-1. Wireless Products Capability/Functional Requirements (Continued)

ID	Requirement	UCR Reference (URC 2008 CH 1)	WLANS	WAB	WLAS	WEI
	data – three devices are required to support all traffic types). The shared access method allows a single wireless WLAS to provide for all traffic types supported (i.e., voice, video, and data – one device provides all three traffic types), on all computer types and/or personal equipment product (PED) to connect to the wireless WLAS.					
18	WEIs may use either method separately or a combination to provide wireless access (see figure 5.3.1-8, access methods for the wireless access layer end item product telephones).	UCR 2008: 5.3.1.7.2.4 (3)				R
19	WEIs or soft clients on workstations acting as WEI shall authenticate to the VoIP system call control. Authentication shall be IAW UCR IA-specified requirements.	UCR 2008: 5.3.1.7.2.4 (4)				R
20	The WEI is associated with the supporting IP telephone switch. The WEI shall be functionally identical to a traditional IP wired telephone and will be required to provide voice features and functionality IAW other UCR specified requirements unless explicitly stated.	UCR 2008: 5.3.1.7.2.4 (5)				R
21	Minimally, all WEIs shall be FIPS 140-2 Level 1 certified.	UCR 2008: 5.3.1.7.2.4 (6)				R
22	If the WEI loses connection with the VoIP switch when using a WLAN, the call will be terminated by the VoIP switch. The termination period shall be determined by the VoIP switch using a configurable time-out parameter with a time-out range of 0-60 seconds; default shall be set to 5 seconds. The subscriber line will be treated as if it were out of service until communication is re-established with the wireless voice end instrument.	UCR 2008: 5.3.1.7.2.4 (7)				R
23	Failure of a WLAS shall not cause the loss of a call as the connection transfers from the primary	UCR 2008 5.3.1.7.2.5 (1)			R	

Table 3-1. Wireless Products Capability/Functional Requirements (Continued)

ID	Requirement	UCR Reference (URC 2008 CH 1)	WLANS	WAB	WLAS	WEI
	to alternate system. However, it may allow a single momentary 5-second delay in voice bearer traffic in both directions of the wireless link as wireless VoIP telephone clients are re-authenticated to the standby system. The 5-second voice delay will not be factored into the overall MOS score.					
24	The WLAS shall support the following maximum number of EIs per Table 5.3.1-8, Maximum Number of EIs Allowed per WLAS, for converged or non-converged access for redundant and non-redundant WLAS; while not degrading any of the individual EIs' voice quality below the specified MOS scores for strategic and tactical situations, in an open air environment at a distance of 100 feet, except for the 5-second re-authentication as stated in item 1, (i.e., Strategic MOS 4.0, Strategic-to-Tactical MOS 3.6, Tactical-to-Tactical MOS 3.2).	UCR 2008 5.3.1.7.2.5 (2)			R	
25	At the point when voice quality degradation occurs, defined as a MOS score below appropriate levels (i.e., Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2), when all telephones are off-hook simultaneously, this becomes the maximum number of telephones and/or other wireless non-voice end item products that the WLAS can support for the WLAS transmitter coverage distance.	UCR 2008 5.3.1.7.2.5 (3)			R	
26	The WLAS shall not drop an active call as the WEI roams from one WLAS transmitter zone into another WLAS transmitter zone.	UCR 2008: 5.3.1.7.2.5 (4)			R	
27	For any of the 802.16 interfaces, the WAB must support any of the following 802.16 standards: a. 802.16d – Part 16: Air Interface for Fixed	UCR 2008: 5.3.1.7.2.6 (1)		R		

Table 3-1. Wireless Products Capability/Functional Requirements (Continued)

ID	Requirement	UCR Reference (URC 2008 CH 1)	WLANS	WAB	WLAS	WEI
	Broadband Wireless Access Systems, or b. 802.16e – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, & Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1.					
28	The maximum number of voice calls transported across the WAB shall be in accordance with section 5.3.1.7.3, traffic engineering. Maximum voice users will be determined by the smallest link size (i.e., Ethernet connection to the WAB or the WAB wireless link speed of the WAB itself).	UCR 2008: 5.3.1.7.2.6 (2)		R		
29	The introduction of a WAB(s) shall not cause the E2E average MOS to fall below appropriate levels (strategic 4.0, strategic-to-tactical 3.6, and tactical-to-tactical 3.2) as measured over any 5-minute time interval.	UCR 2008: 5.3.1.7.2.6 (3)		R		
30	The introduction of a WAB(s) shall not exceed the E2E digital ber requirement of less than 1 error in 1x10 ⁻⁸ (averaged over a 9-hour period).	UCR 2008: 5.3.1.7.2.6 (4)		R		
31	The introduction of a WAB(s) shall not degrade secure transmission for secure end products as defined in UCR 2008 section 5.2.6, DoD Secure Communications Devices (DSCDS).	UCR 2008: 5.3.1.7.2.6 (5)		R		
32	The WAB shall transport all call control signals transparently on an E2E basis.	UCR 2008: 5.3.1.7.2.6 (6)		R		
33	The addition of a WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 MS for each WAB used, averaged over any 5-minute period.	UCR 2008: 5.3.1.7.2.6 (7)		R		

Table 3-1. Wireless Products Capability/Functional Requirements (Continued)

ID	Requirement	UCR Reference (URC 2008 CH 1)	WLANS	WAB	WLAS	WEI
34	The addition of the WAB shall not increase the LAN jitter requirements previously specified in this section.	UCR 2008: 5.3.1.7.2.6 (8)		R		
35	The WLAS/WAB combination must meet all the requirements for access and bridging.	UCR 2008: 5.3.1.7.2.6 (8)		R	R	
36	The WAB(s) and/or WLAS/WAB shall support service class tagging/qos as previously specified in this section.	UCR 2008: 5.3.1.7.2.6 (8)-1		R	R	
37	The WABs may support F/FO calls, I/PR, and non-mission critical calls. All calls must meet other specified performance requirements for these users.	UCR 2008: 5.3.1.7.2.6 (8)-2		R	R	

LEGEND:

ASLAN	Assured Services Local Area Network	O	Optional
BER	Bit Error Rate	QoS	Quality of Service
C	Conditional	R	Required
DISA	Defense Information Systems Agency	STIG	Security Technical Implementation Guides
DoD	Department of Defense	UCR	Unified Capability Requirement
DSCP	Differentiated Services Code Point	VoIP	Voice over Internet Protocol
E2E	End to End	WAB	Wireless Access Bridge
FIPS	Federal Information Processing Standards	WEI	Wireless End Instrument
F/FO	Flash/ Flash Override	WIDS	Wireless Intrusion detection system
IP	Internet Protocol	Wi-Fi	Wireless Fidelity
IPv6	Internet Protocol version 6	WLANS	Wireless Local Area Networks
LAN	Local Area Network	WLAS	Wireless LAN Access System
MOS	Mean Opinion Score	WPA2	Wireless Protocol Authentication 2

This page intentionally left blank.