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

IN REPLY REFER TO: Joint Interoperability Test Command (JTD) 1 March 2018

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the ForeScout Technologies Inc. CounterACT NAC V7.0

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Change 1," June 2015
(c) through (d), see Enclosure 1

1. **Certification Authority.** Reference (a) establishes the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for Department of Defense Information Network (DoDIN) products, Reference (b).

2. **Conditions of Certification.** ForeScout Technologies Inc. CounterACT Network Control Access (NAC) V7.0 is hereinafter referred to as the System Under Test (SUT). The SUT meets the requirements of the Unified Capabilities Requirements (UCR) 2013 Change 1, Reference (b) and is certified for joint use as a NAC with the conditions described in Table 1. This certification expires upon changes that could affect interoperability, but no later than the expiration date specified in the DoDIN Approved Products List (APL) memorandum.

Table 1. Conditions

Description	Operational Impact	Remarks
UCR Waivers		
None		
Conditions of Fielding		
None		

Table 1. Conditions

Description		Operational Impact	Remarks
TDR#	**Open Test Discrepancies**		
002	IP6-000050: The system shall provide the same (or equivalent) functionality in IPv6 operation as it provides in IPv4 operation consistent with the requirements in the UCR for its APL category. (Not Met) ForeScout CounterAct does not have the same functionality with IPv6 as it does with IPv4.	Minor with POA&M	The SUT could not integrate with active directory using an IPv6 address. (See note.)
003	IP6-000470: The product shall support manual assignment of IPv6 addresses. (Not Met) ForeScout CounterAct does not support manual assignment of IPv6 addresses.	Minor with POA&M	The vendor SUT does not function properly when a manual IPv6 address is configured. (See note.)

NOTE(S): DISA accepted the vendor's POA&M and adjudicated this discrepancy as having a Minor operational impact. Mitigation: The IPv6 feature can be disabled since the system is not currently using IPv6 for network management communications.

LEGEND:

APL	Approved Products List	SUT	System Under Test
DISA	Defense Information Systems Agency	TDR	Test Discrepancy Report
IP	Internet Protocol	UCR	Unified Capabilities Requirements
POA&M	Plan of Action and Milestones	v	Version

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status, Table 3 provides the Capability Requirements and Functional Requirements status, and Table 4 provides a DoDIN APL product summary.

Table 2. Interface Status

Interface (See note 1.)	Applicability (R), (O), (C)	Status (Met, Partially Met, Not Met, Not Tested)	Remarks
Product Interfaces			
10BASE-X	R	Met	
100BASE-X	R	Met	
1000BASE-X	O	Met	
10GBASE-X	O	Not Tested	(See note 2.)
40GBASE-X	O	Not Tested	(See note 2.)
100GBASE-X	O	Not Tested	(See note 2.)

NOTE(S):
1. The UCR 2013 Change 1, Section 13 does not identify individual interface requirements for security devices. The SUT must minimally provide Ethernet interfaces that meet the requirements in Section 2.7.1.
2. The SUT does not support this (conditional or optional) interface.

LEGEND:

Base-X	Mbps Baseband Ethernet over Fiber or Copper	R	Required
GBASE-X	Gbps Ethernet over Fiber or Copper	SUT	System Under Test
Mbps	Megabits per second	UCR	Unified Capabilities Requirements
O	Optional		

Table 3. Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (See note 1.)	UCR 2013 Change 1 Reference	Status (Met, Partially Met, Not Met, Not Tested)
1	Cybersecurity (R)	See note.2	Partially Met
2	IA Requirements for SD (R)	4.2	Partially Met
3	IPv6 (R)	5.2	Partially Met
4	Security Device Requirements (R)	13.2	Met

NOTE(S):
1. The annotation of "required" refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. Cybersecurity testing is based on DISA STIG/SRGs. A TSSAP-led Cybersecurity test team tested Security and published the results in a separate report, Reference (d). Cybersecurity testing for Security Devices was also conducted

LEGEND:

CR	Capability Requirements	R	Required
FR	Functional Requirements	SRG	Security Requirements Guide
JITC	Joint Interoperability Test Command	STIG	Security Technical Implementation Guide
ID	Identification	TSSAP	Telecommunications Systems Security Assessment Program
IPv6	Internet Protocol version 6	UCR	Unified Capabilities Requirements

Table 4. DoDIN APL Product Summary

Product Identification			
Product Name	ForeScout CounterACT NAC		
Software Release	V7.0		
DoDIN Product Type(s)	Network Access Control		
Product Description	The ForeScout CounterACT NAC solution, referred to as CounterACT NAC for short, is an agentless visibility and control solution that also includes the ability to protect network resources from threats such as malware and worms.		
DoDIN Certified Function	**Component/ Sub-Component Name (See note.)**	**Tested Version**	**Remarks**
Network Access Control	**CounterACT Enterprise Manager CEM-10**	V7.0	Management Server
	CounterACT Appliance CT-R	V7.0	Sensor
	CounterACT Appliance CT-2000	V7.0	Sensor
	CounterACT Appliance CT-10000	V7.0	Sensor
	CounterACT Appliance VCT-1000	V7.0	Virtual Sensor

NOTE(S): Components bolded and underlined were tested by Telecommunications Systems Security Assessment Program at JBSA Lackland, Texas.

LEGEND:

APL	Approved Products List	DoDIN	Department of Defense Information Network
CEM	CounterACT Enterprise Manager	NAC	Network Access Control
CT	CounterACT		

4. **Test Details.** This certification is based on interoperability testing, Defense Information Systems Agency (DISA) adjudication of open Test Discrepancy Reports (TDRs), review of the vendor's Letters of Compliance (LoC), and DISA adjudication of open Test Discrepancy Reports (TDRs) for inclusion on the DoDIN APL. the Telecommunications Systems Security Assessment Program (TSSAP) at JBSA Lackland, Texas, conduced testing from 4 December 2017 through 15 December 2017, using test procedures derived from Reference (c). DISA completed adjudication of outstanding test discrepancies on 25 January 18. Review of the vendor's LoC was completed on 10 November 17. TSSAP-led Cybersecurity (CS) test teams conducted CS testing and published the results in a separate report, Reference (d). Enclosure 2

documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

5. **Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users 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 https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the Cybersecurity Assessment Package (CAP) that contains the approved configuration and deployment guide must be requested directly from the Approved Products Certification Office (APCO) by e-mail: disa.meade.ie.list.approved-products-certification-office@mail.mil. All associated information is available on the DISA APCO website located at http://www.disa.mil/network-services/UCCO.

6. **Point of Contact (POC).** TSSAP testing POC: Mr. Ruben Almaraz; commercial telephone 210-925-3538; DSN 945-3238; e-mail address: ruben.almaraz@us.af.mil. JITC certification POC: Mr. Keith Watson; commercial phone 301-225-9460; e-mail address: keith.d.watson2.civ@mail.mil; mailing address: Joint Interoperability Test Command, ATTN: JTD1 (Mr. Keith Watson), 6910 Cooper Ave., Fort Meade, Maryland 20755. The APCO tracking number for the SUT is 1717301.

FOR THE COMMANDER:

CLARK.BRADLEY.ALAN.1231466564 Digitally signed by CLARK.BRADLEY.ALAN.1231466564 Date: 2018.03.01 13:45:51 -07'00'

3 Enclosures a/s

for RIC HARRISON
Chief
Networks/Communications and UC Division

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

ADDITIONAL REFERENCES

(c) Joint Interoperability Test Command, "Unified Capabilities Security Device Test Procedures Version 1.0 for Unified Capabilities Requirements (UCR) 2013 Change 1," June 2015.
(d) Joint Interoperability Test Command, “Cybersecurity Assessment Report for ForeScout Technologies Inc CounterACT NAC Version 7.0 SP 2.8.0 (Tracking Number 1717301)” Draft, December 2017

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The ForeScout Technologies Inc. CounterACT NAC v7.0 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	United States Marine Corps
Sponsor Point of Contact	Bill Moses, Cybersecurity Architect, email: bill.moses@usmc.mil
Vendor Point of Contact	Herbert Markle, Senior Evaluator, email: markle_herbert@bah.com
System Name(s)	ForeScout Technologies Inc., CounterACT NAC
Increment and/or Version	Version 7.0
Product Category	Network Access Control
System Background	
Previous certifications	Previous JITC certification (same release) or host cert if this is an extension
Tracking	
APCO ID	1717301
System Tracking Program ID	System # 6351, Test Activity # 15765
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Change 1, Section 13
Remarks	None
Test Organization(s)	TSSAP
LEGEND: APCO Approved Products Certification Office NAC Network Access Control	 STP System Tracking Program SW Software

2. SYSTEM DESCRIPTION. The Department of Defense (DoD) Information Network (DoDIN) services include transport, data, voice, video, messaging, and other capabilities along with ancillary enterprise services. A key component of the DoDIN transport is the Security Device (SD). Security Devices are generally considered to be "cybersecurity and cybersecurity-enabled information technology (IT) Information Assurance Products" in accordance with Department of Defense (DoD) Directive (DoDD) 8500.1. These cybersecurity and cybersecurity-enabled products requirements include network-based Firewalls (FWs), Intrusion Prevention Systems (IPSs), Virtual Private Network (VPN) servers, and Network Access Controllers (NACs), for example. More information on Security Devices can be found in Section 13, Security Devices.

The ForeScout CounterACT NAC solution, referred to as CounterACT NAC for short, is an agentless visibility and control solution that also includes the ability to protect network resources from threats such as malware and worms. CounterACT NAC integrates with compatible switches and other network infrastructure from more than thirty switch and wireless vendors in order to enforce access control policies per physical port. This allows both trusted users and network guests to remain productive while protecting critical network resources and sensitive data.

The following subparagraphs offer brief descriptions of the CounterACT NAC components (provided by ForeScout Technologies Inc. data sheets) listed by tracking number.

Component 1. CounterACT Enterprise Manager CEM-10

Component 2. CounterACT Appliance CT-R

Component 3. CounterACT Appliance CT-2000

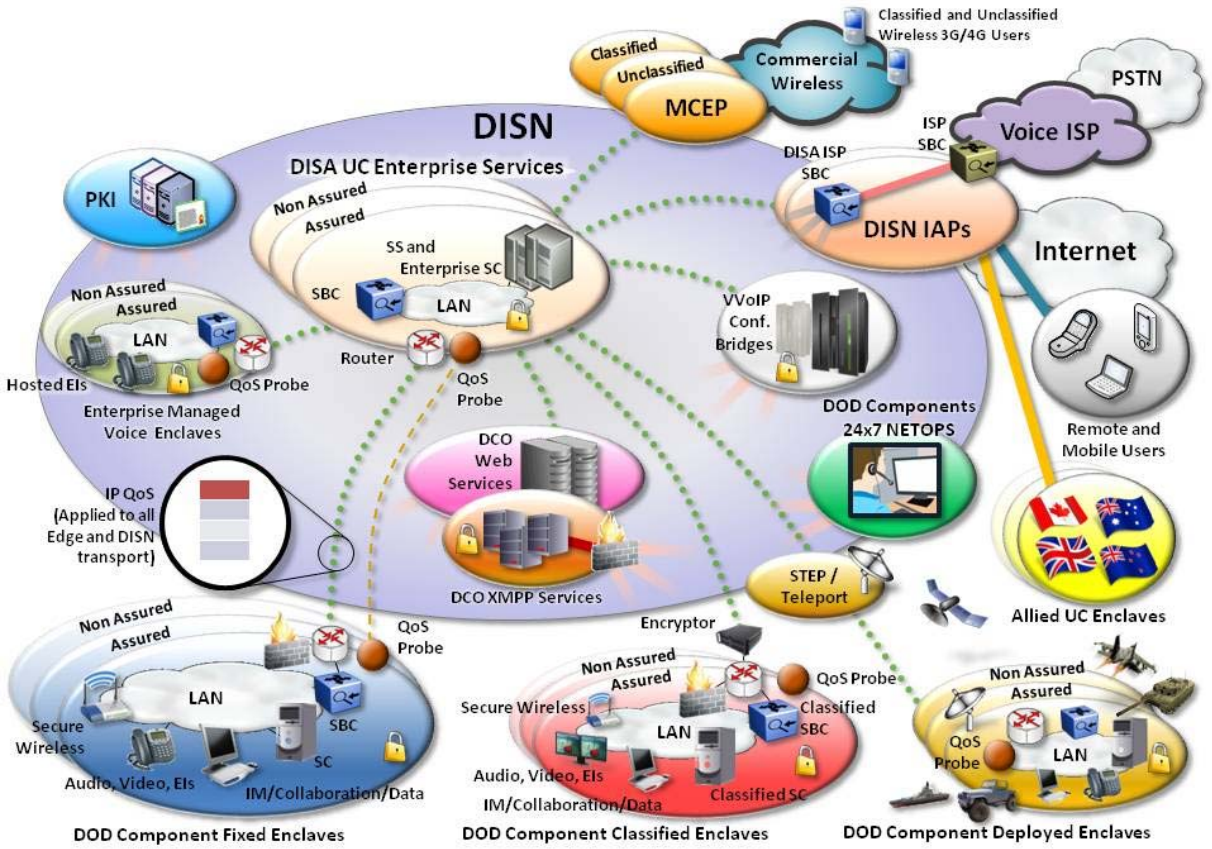
Component 4. CounterACT Appliance CT-10000

Component 5. CounterACT Appliance VCT-1000

3. OPERATIONAL ARCHITECTURE. The DoDIN architecture is a two-level network hierarchy consisting of Defense Information Systems Network backbone switches and Service/Agency installation switches. The DoD Chief Information Officer and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The DoDIN architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the Notional Operational DoDIN Architecture in which the SUT may be used. Figure 2-2 depicts the DoDIN Security Device Functional Reference Model.

4. TEST CONFIGURATION. The test team tested the SUT at the Telecommunications Systems Security Assessment Program (TSSAP), JBSA-Lackland San Antonio, Texas in a manner and configuration similar to that of a notional operational environment depicted in Figure 2-1. The test team verified the SUT's required functions and features using the test configuration depicted in Figure 2-2. The test team conducted interoperability testing of the NAC components by testing the SUT with different vendor DoDIN APL certified products as illustrated in Figure 2-2. Cybersecurity testing used the same configuration.

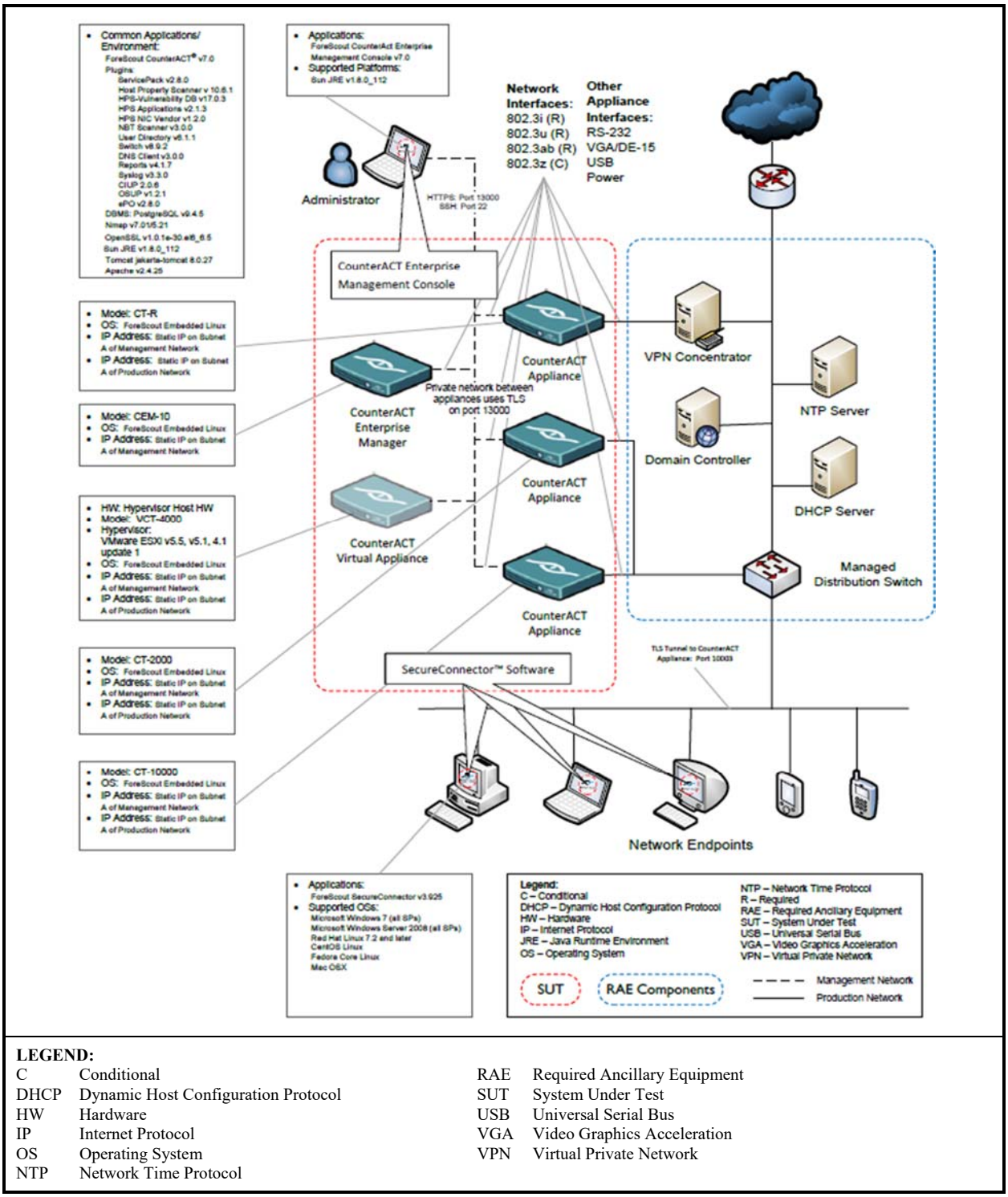
5. METHODOLOGY. TSSAP conducted testing of the Network Access Controller (NAC) using requirements derived from the UC Requirements (UCR) 2013, Change 1, Reference (b), and the test procedures, Reference (c). In addition to testing, an analysis of the vendor's Letters of Compliance (LoC) verified that letter "R" requirements have been met. Any discrepancies noted were documented in Test Discrepancy Reports (TDRs). The vendor submitted Plan of Action and Milestones (POA&M) as required. Any new discrepancy noted in the operational environment will be evaluated for impact on the existing interoperability certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor POA&M, which will address all new critical TDRs within 120 days of identification.



LEGEND:

DCO	Defense Connection Online
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
EI	End Instrument
IAP	Internet Access Point
IM	Instant Messaging
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MCEP	Multi Carrier Entry Point
NETOPS	Network Operations
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SBC	Session Border Controller
SC	Session Controller
SS	Softswitch
STEP	Standardized Tactical Entry Point
UC	Unified Capabilities
VVoIP	Voice and Video over IP
XMPP	Extensible Messaging and Presence Protocol

Figure 2-1. Notional DoDIN Architecture



LEGEND:

C	Conditional	RAE	Required Ancillary Equipment
DHCP	Dynamic Host Configuration Protocol	SUT	System Under Test
HW	Hardware	USB	Universal Serial Bus
IP	Internet Protocol	VGA	Video Graphics Acceleration
OS	Operating System	VPN	Virtual Private Network
NTP	Network Time Protocol		

Figure 2-2. SUT Interoperability Test Configuration

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The interface, Capability Requirements (CR) and Functional Requirements (FR), Cybersecurity (CS), Internet Protocol version 6 (IPv6), and other requirements for Security Devices are defined by UCR 2013 Change 1, Sections 5 and 13. Please refer to Table 3-2 for a detailed list of requirements.

a. The UCR 2013, Change 1, Section 5.2 includes the IPv6 Requirements.

(1) Section 5.2.1 of UCR 2013 provided the detailed IPv6 product requirements for SD: Maximum Transmission Unit, Flow Label, Address, Neighbor Discovery, Stateless Address Autoconfiguration and Manual Address Assignment, Internet Control Message Protocol, Traffic Engineering, IP Version Negotiation. The SUT partially met this requirement. DISA accepted the vendor's POA&M and adjudicated the discrepancy as having a minor operational impact, as noted in Table 1.

(2) Section 5.2.2 of UCR 2013 provided the [Mapping of RFCs to DoDIN Profile Categories]. The SUT met this requirement with testing.

b. The UCR 2013, Change 1, Section 13.2 includes the Security Device Requirements.

(1) Section 13.2.1 of UCR 2013 provided the conformance requirements for Virtual Private Network (VPN). This section is applicable to only a VPN. This requirement is not applicable to a NAC and was not tested.

(2) Section 13.2.2 of UCR 2013 provided the general requirements for Firewall (FW), Intrusion Prevention System (IPS), VPN, Network Access Control (NAC), and Wireless Intrusion Detection System (WIDS). The SUT met this requirement with testing and the vendor's LoC.

(3) Section 13.2.3 of UCR 2013 provided the performance requirements for FW, IPS, and VPN. Security devices are intended to mitigate the threats enclaves face from external sources while permitting transmission of legitimate traffic in both directions. Performance tests attempt to validate a security device's ability to maintain that legitimate traffic stream while the network is under attack. This requirement is not applicable to a NAC and was not tested

(4) In addition to Section 4, the UCR 2013 Section 13.2.4 also specifies functional requirements for "security-device-unique" products such as network-based FWs, IPSs, VPN concentrators, Integrated Security System (ISSs), WIDS, and NACs. The SUT met this requirement with testing.

(5) Section 13.2.4.1.1 of UCR 2013 provided policy requirements for FW and VPN. This section identifies the need for a security device to respond to policy-based actions set by a System Administrator. This section is applicable to only FW or VPN. This requirement is not applicable to a NAC and was not tested.

(6) Section 13.2.4.1.2 of UCR 2013 provided filtering requirements for FW to perform basic filtering functions. The security device's controlled interface must support and filter communications protocols/services from outside the perimeter of the interconnected Information Systems (ISs) according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications). Filtering is defined as having the ability to block on a per-interface basis, defaulting to block, and defaulting to disabled, if supported on the security device itself. This section is applicable to only FW or VPN. This requirement is not applicable to a NAC and was not tested.

(7) Section 13.2.4.2 of UCR 2013 provided functionality requirements for IPS. This section is applicable to only IPSs. This requirement is not applicable to a NAC and was not tested.

(8) Section 13.2.4.3 of UCR 2013 listed requirements for ISS systems that provide the functionality of more than one cybersecurity device in one integrate device. This section is applicable to only ISSs. This requirement is not applicable to a NAC and was not tested.

(9) Section 13.2.4.5 of UCR 2013 provided requirements for NAC. The NAC attempts to control access to a network with policies including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. A system is composed of many elements and is not a single device. This section is applicable for only NAC. The SUT met this requirement with testing and the vendor's LoC.

7. Hardware/Software/Firmware Version Identification. Table 3-3 provides the SUT components' hardware, software, and firmware tested. TSSAP, JBSA-Lackland, Texas tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

8. TESTING LIMITATIONS. JITC's test team noted the following testing limitations including the impact on the certification: **None.**

9. CONCLUSION(S). The SUT meets the interoperability requirements for a NAC in accordance with the UCR and is certified for joint use with other DoDIN Products listed on the DoDIN APL.

DATA TABLES

Table 3-1. Interface Status

Interface (See note 1.)	Applicability (R), (O), (C)	Status (Met, Partially Met, Not Met, Not Tested)	Remarks
Product Interfaces			
10BASE-X	R	Met	
100BASE-X	R	Met	
1000BASE-X	O	Met	
10GBASE-X	O	Not Tested	(See Note 2.)
40GBASE-X	O	Not Tested	(See Note 2.)
100GBASE-X	O	Not Tested	(See Note 2.)

NOTE(S):
1. The UCR 2013 Change 1, Section 13 does not identify individual interface requirements for security devices. The SUT must minimally provide Ethernet interfaces that meet the requirements in Section 2.7.1.
2. The SUT does not support this (conditional or optional) interface.

LEGEND:

Base-X	Mbps Baseband Ethernet over Fiber or Copper	R	Required
GBASE-X	Gbps Ethernet over Fiber or Copper	SUT	System Under Test
Mbps	Megabits per second	UCR	Unified Capabilities Requirements
O	Optional		

Table 3-2. Capability and Functional Requirements and Status

CR/FR ID	Capability/ Function	Applicability (See note 1.)	UCR 2013 Change 1 Reference	Status (Met/Partially Met/ Not Met/Not Tested)
1	**Internet Protocol Version 6 Requirements**			
	Product Requirements	R	5.2.1	Partially Met (See note 2.)
	Mapping of RFCs to DoDIN Profile Categories	R	5.2.2	Met
2	**Security Device Requirements**			
	Conformance	R	13.2.1	Not Tested (See note 3.)
	General	R	13.2.2	Met
	Performance	R	13.2.3	Not Tested (See note 4.)
	Functionality	R	13.2.4	Met
	FW/VPN	R	13.2.4.1	Not Tested (See note 5.)
	IPS	R	13.2.4.2	Not Tested (See note 6.)
	ISS	R	13.2.4.3	Not Tested (See note 7.)
	NAC	R	13.2.4.5	Met

NOTE(S):
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each requirement is provided in UCR 2013, Change 1, Reference (b). The SUT does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements.
2. Section 5.2.1 was partially met. DISA accepted the vendor's POA&M and adjudicated the discrepancy as having a minor operational impact, as noted in Table 1.
3. Section 13.2.1 is applicable to only VPN.\
4. Section 13.2.3 is applicable to only Firewall, IPS, and VPN.
5. Section 13.2.4.1 is applicable to only Firewall and VPN.
6. Section 13.2.4.2 is applicable to only IPS.
7. Section 13.2.4.3 is applicable to only ISS.

Table 3-2. Capability and Functional Requirements and Status (continued)

LEGEND:

CR	Capability Requirements	NAC	Network Access Control
CYB	Cybersecurity	POA&M	Plan of Action and Milestones
DISA	Defense Information Systems Agency	R	Required
FR	Functional Requirements	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements
IP	Internet Protocol	v	Version
IPS	Intrusion Prevention System	VPN	Virtual Private Network
ISS	Integrated Security System		

Table 3-3. SUT Hardware/Software/Firmware Version Identification

Component (See note 1.)	Release	Sub-component (See note.)	Description
ForeScout Technologies CounterACT NAC	7.0	**CEM-10**	Management Server
		CT-R	CounterACT Appliance
		CT-2000	CounterACT Appliance
		CT-10000	CounterACT Appliance
		VCT-1000	CounterACT Virtual Appliance

NOTE(S): Components bolded and underlined were tested by Telecommunications Systems Security Assessment Program.

LEGEND:
NAC Network Access Control

Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification

System Name	Software Release	Function
Required Ancillary Equipment		
Syslog NG	4.3	SYSLOG
DC1	Windows 2008R2 DoD Baseline	Active Directory
Test Network Components		
Workstation	Windows 10 DoD Baseline	Management PC
Workstation	Windows 10 DoD Baseline	User PC
Workstation	Windows 10 DoD Baseline	User PC
Switch (Cisco 3560-X)	12.2.55se1	LAN Switch
Switch (Cisco 3750-X)	12.2.55se1	LAN Switch
Ixia	8.10.10466ea	Traffic Generation Appliance

LEGEND:

DC	Device Control	R	Release
DoD	Department of Defense	RADIUS	Remote Authentication Dial - In User Service
HP	Hewlett Packard	RHEL	Red Hat Enterprise Linux
LAN	Local Area Network	SP1	Service Pack 1
N/A	Not Applicable	SYSLOG	System Log
NG	Next Generation	TGA	Traffic Generation Appliance
PC	Personal Computer		