



DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY
REFER
TO:

Joint Interoperability Test Command (JITE)

14 Nov 12

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Special Interoperability (IO) Test Certification of the McAfee Network Security Platform (NSP) (M-8000, M-6050, M-4050, M-3050, M-2950, M-2850, M-2750, M-1450, M-1250) Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) with software release 6.1.15.33

References: (a) DoD 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 (f), see Enclosure

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for Interoperability (IO) test certification.
2. The McAfee NSP (M-8000, M-6050, M-4050, M-3050, M-2950, M-2850, M-2750, M-1450, M-1250) with software release 6.1.15.33 hereinafter referred to as the System Under Test (SUT), meets all the critical IO requirements for an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) and is certified for joint use within the Defense Information System Network (DISN). The certification status of the SUT will be verified during operational deployment. Any new discrepancies noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of the Defense Information Systems Agency (DISA) via a vendor Plan of Action and Milestones (POA&M) which address all new critical Technical Deficiency Reports (TDRs) within 120 days of identification. Testing was conducted using security device requirements derived from the Unified Capabilities Requirements (UCR), Reference (c), and Test Procedures, Reference (e). No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that affect IO, but no later than three years from the date of the signed Department of Defense (DoD) Unified Capabilities (UC) Approved Product List (APL) approval memorandum 27-Sep-2011.
3. The original certification is based on interoperability (IO) testing conducted by JITC, Indian Head, Maryland, review of the vendor's Letters of Compliance (LoC), and DISA Information Assurance (IA) Certification Authority (CA) approval of the IA configuration. IO testing was conducted by JITC from 03-Jan-2011 through 28-Jan-2011. The DISA CA has reviewed the IA Assessment Report for the SUT (Reference (f)) and based on the findings in the report provided a positive recommendation. JITC issued the original IO certification on 13-Sep-2011. The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation. The JITC certifies the SUT as meeting the UCR for IDS/IPS.

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the McAfee Network Security Platform (M-8000, M-6050, M-4050, M-3050, M-2950, M-2850, M-2750, M-1450, M-1250) IDS/IPS with software release 6.1.15.33

4. The extension of this certification is based upon Desktop Reviews (DTRs) 1& 2. McAfee requested DTR 1 for a change in software from code version 6.1.15.12 to 6.1.15.17 and DTR 2 for FIPS 140-2 verification. JITC determined that V&V testing was required to address Common Criteria requirements and FIPS-140-2 certification prior to approval. In addition, bug fixes were applied to address logging of users who Common Access Card (CAC) does not match an associated account on the Network Security Manager (NSM), report generation problems and passwords lockout issues. JITC conducted V&V testing from 07-May-2012 through 11-May-2012 and DTR 1 & 2 were successfully verified. The DISA CA concurred with JITC's determination and provided a positive recommendation on DTR 1&2 on 03-Jul-2012. Therefore, DTR 1&2 are approved by JITC and the SUT is now certified for use in the DISN.

5. The interface, component status of the SUT, and Capability Requirements (CR) and Functional Requirements (FR) is listed in Table 1 and Table 2. The threshold CR/FR requirements for security devices are established by Section 5.8 of Reference (c) and were used to evaluate the IO of the SUT.

Table 1. SUT Interface Interoperability Status

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Status	Remarks (See note 3.)										
IPS															
10Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	All Security Systems										
100Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	All Security Systems										
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	All Security Systems										
10GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	Met	M-8000, M-6050, M-4050, M-3050										
40GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	NA	Not Supported										
100GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	NA	Not Supported										
<p>NOTES:</p> <p>1. UCR did not identify individual interface requirements for security devices. SUT must minimally provide an Ethernet interface (one of the listed).</p> <p>2. CR/FR requirements are contained in Table 2. CR/FR numbers represent a roll-up of UCR requirements.</p> <p>3. SUT will meet applicable standards for interface provided.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">CR Capability Requirement</td> <td style="width: 50%;">NA Not Applicable</td> </tr> <tr> <td>FR Functional Requirement</td> <td>SUT System Under Test</td> </tr> <tr> <td>ID Identification</td> <td>UCR Unified capabilities Requirements</td> </tr> <tr> <td>IPS Intrusion Protection System</td> <td>Y Yes</td> </tr> <tr> <td>N No</td> <td></td> </tr> </table>						CR Capability Requirement	NA Not Applicable	FR Functional Requirement	SUT System Under Test	ID Identification	UCR Unified capabilities Requirements	IPS Intrusion Protection System	Y Yes	N No	
CR Capability Requirement	NA Not Applicable														
FR Functional Requirement	SUT System Under Test														
ID Identification	UCR Unified capabilities Requirements														
IPS Intrusion Protection System	Y Yes														
N No															

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/ Function	Applicability (See note 1.)	UCR Reference	Status	Remarks												
1	Conformance Requirements																
	Conformance Standards	Required	5.8.4.2	Met													
2	Information Assurance Requirements																
	General Requirements	Required	5.8.4.3.1	Met													
	Authentication	Required	5.8.4.3.2	Met													
	Configuration Management	Required	5.8.4.3.3	Met													
	Alarms & Alerts	Required	5.8.4.3.4	Met													
	Audit and Logging	Required	5.8.4.3.5	Met													
	Integrity	Required	5.8.4.3.6	Met													
	Documentation	Required	5.8.4.3.7	Met													
	Cryptography	Required (See note 2.)	5.8.4.3.8	Met	IPSec Not Supported see note 3												
	Security Measures	Required	5.8.4.3.9	Met													
	System and Communication Protection	Required	5.8.4.3.10	Met													
	Other Requirements	Required	5.8.4.3.11	Met													
	Performance	Required	5.8.4.3.12	Met													
3	Functionality																
	Policy	Required	5.8.4.4.1	NA	FW & VPN Only												
	Filtering	Required	5.8.4.4.2	NA	FW Only												
4	IPS Functionality																
	IPS Security Device Requirements	Required (See note 4.)	5.8.4.5	Met	IDS/IPS Only												
<p>NOTES:</p> <ol style="list-style-type: none"> Criticality represents high level roll-up of the CR/FR area. Cryptography is optional with the exception that all outgoing communications are encrypted. Outgoing communications are encrypted with TLS. IPS functionality only applies to IPS products. Requirements are not applicable to firewalls or VPN concentrators. <p>LEGEND:</p> <table> <tr> <td>IP</td> <td>Internet Protocol</td> <td>IPS</td> <td>Intrusion Prevention System</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>IPSEC</td> <td>Internet Protocol Security</td> <td></td> <td></td> </tr> </table>						IP	Internet Protocol	IPS	Intrusion Prevention System	FW	Firewall	VPN	Virtual Private Network	IPSEC	Internet Protocol Security		
IP	Internet Protocol	IPS	Intrusion Prevention System														
FW	Firewall	VPN	Virtual Private Network														
IPSEC	Internet Protocol Security																

5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes IO information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive IO status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/.gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to the Defense Switch Network (DSN) testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. All associated data is available on the Defense Information Systems Agency Unified Capability Coordination Office (UCCO) website located at

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the McAfee Network Security Platform (M-8000, M-6050, M-4050, M-3050, M-2950, M-2850, M-2750, M-1450, M-1250) IDS/IPS with software release 6.1.15.33

<https://aplits.disa.mil>.

6. The JITC testing and certification point of contact is Mr. Kevin Holmes, JITC, commercial 301-743-4300; e-mail address is Timothy.K.Holmes.civ@mail.mil. The JITC's mailing address is 3341 Strauss Avenue, Suite 236, Indian Head, Maryland 20640-5149. The Unified Capabilities Certification Office tracking number is 1013901.

FOR THE COMMANDER:



for BRADLEY A. CLARK
Acting Chief
Battlespace Communications Portfolio

Enclosures a/s

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the McAfee Network Security Platform (M-8000, M-6050, M-4050, M-3050, M-2950, M-2850, M-2750, M-1450, M-1250) IDS/IPS with software release 6.1.15.33

Distribution (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ

U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DoD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68

US Army, ATTN: Mr. Cary Rook, Transport Services Branch Chief, 423 22nd Street, Bldg 21715, Fort Gordon, GA 30905-5832, DSN 773-7975, Cary.Rook@us.army.mil

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 1," 22 January 2010.
- (d) Department of Defense Instruction 8100.04, "Department of Defense (DoD) Unified Capabilities (UC)", December 9, 2010.
- (e) Joint Interoperability Test Command, "Security Device Test Procedures," March 2011.
- (f) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of the McAfee Network Security Platform (M-8000, M-6050, M-4050, M-3050, M-2950, M-2850, M-2750, M-1450, M-1250) IDS/IPS with software release 6.1.15.33 . (TN1013901)," April 2011.