



# DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY  
REFER  
TO:

Joint Interoperability Test Command (JTE)

**26 Mar 13**

## MEMORANDUM FOR DISTRIBUTION

**SUBJECT:** Extension of the Special Interoperability (IO) 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/Intrusion Prevention System (IDS/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 IDS/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 (TDR) 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 Approved Product List (APL) approval memorandum 27 Sep 2011.
3. The original certification is based on 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

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

Accreditation Process (DIACAP) accreditation. The JITC certifies the SUT as meeting the UCR for IDS/IPS.

4. The extension of this certification is based upon Desktop Reviews (DTRs) 1, 2, and 3. 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 Federal Information Processing Standards (FIPS) Publication 140-2 compliance verification. JITC determined that Verification and Validation (V&V) testing was required to address Common Criteria requirements and FIPS140-2 certification prior to approval. In addition, bug fixes were applied to address logging of users whose 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 DTRs 1 and 2 were successfully verified. McAfee requested DTR 3 to verify the capability of NSM to use the Delegated Trust Mode for Online Certificate Status Protocol. JITC conducted V&V testing on 22 Feb 2013 and verified McAfee was successfully able to close these findings. The DISA CA concurred with JITC's determination and provided a positive recommendation on DTRs 1 and 2 on 03 Jul 2012 and DTR 3 on 12 Mar 2013. Therefore, DTRs 1, 2, and 3 are approved by JITC and the SUT is now certified for use in the DISN.

5. The interface IO status of the SUT, Capability Requirements (CR), and Functional Requirements (FR) are listed in Tables 1 and 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.)
<b>IPS</b>					
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-
40GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	NA	Not Supported

**Table 1. SUT Interface Interoperability Status (cont)**

INTERFACE	CRITICAL (See note 1.)	UCR Reference	THRESHOLD CR/FR REQUIREMENTS (See note 2.)	STATUS	REMARKS (See note 3.)												
100GBase-X	No	5.3.2.4 / 5.3.3.10.1.2	1-4	NA	Not Supported												
<p><b>NOTES:</b></p> <p>1. UCR did not identify individual interface requirements for security devices. SUT must minimally provide an Ethernet interface.</p> <p>2. CR/FR requirements are contained in Table 2 and CR/FR numbers represent a roll-up of UCR requirements.</p> <p>3. SUT will meet applicable standards for interface provided.</p> <p><b>LEGEND:</b></p> <table> <tr> <td>CR</td> <td>Capability Requirement</td> <td>NA</td> <td>Not Applicable</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>IPS</td> <td>Intrusion Prevention System</td> <td>UCR</td> <td>Unified capabilities Requirements</td> </tr> </table>						CR	Capability Requirement	NA	Not Applicable	FR	Functional Requirement	SUT	System Under Test	IPS	Intrusion Prevention System	UCR	Unified capabilities Requirements
CR	Capability Requirement	NA	Not Applicable														
FR	Functional Requirement	SUT	System Under Test														
IPS	Intrusion Prevention System	UCR	Unified capabilities Requirements														

**Table 2. SUT Capability Requirements and Functional Requirements Status**

CR/FR ID	CAPABILITY/FUNCTION	APPLICABILITY (See note 1.)	UCR Reference	STATUS	REMARKS
1	<b>Conformance Requirements</b>				
	Conformance Standards	Required	5.8.4.2	Met	
2	<b>Information Assurance Requirements</b>				
	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 and 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	<b>Functionality</b>				
	Policy	Required	5.8.4.4.1	NA	FW and VPN Only
	Filtering	Required	5.8.4.4.2	NA	FW Only

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

**Table 2. SUT Capability Requirements and Functional Requirements Status (cont)**

<b>4</b>	<b>IPS Functionality</b>				
	IPS Security Device Requirements	Required (See note 4.)	5.8.4.5	Met	IDS/IPS Only
<b>NOTES:</b>					
1. Criticality represents high level roll-up of the CR/FR area.					
2. Cryptography is optional with the exception that all outgoing communications are encrypted.					
3. Outgoing communications are encrypted with Transport Layer Security.					
4. IPS functionality only applies to IPS products. Requirements are not applicable to firewalls or VPN concentrators.					
<b>LEGEND:</b>					
CR	Capability Requirement	IPS	Intrusion Prevention System		
FR	Functional Requirement	IPSec	Internet Protocol Security		
FW	Firewall	NA	Not Applicable		
ID	Identification	UCR	Unified Capabilities Requirements		
IDS	Intrusion Detection System	VPN	Virtual Private Network		

6. 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>. Information related to the Defense Switch Network (DSN) testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitic.fhu.disa.mil/tssi>. All associated data is available on the DISA Unified Capability Coordination Office (UCCO) website located at <https://aplits.disa.mil>.

7. JITC testing and certification point of contact is Ms. Baotram (BT) Tran, JITC, commercial 301-743-4319; e-mail address is Baotram.Tran.civ@mail.mil. JITC's mailing address is 3341 Strauss Avenue, Suite 236, Indian Head, Maryland 20640-5149. The UCCO tracking number for the SUT is 1013901.

FOR THE COMMANDER:

Enclosures a/s

  
for RICHARD A. MEADOR  
Chief  
Battlespace Communications Portfolio

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):

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, MARCORSSYSCOM, 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

## **ADDITIONAL REFERENCES**

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 1," 22 January 2010.
- (d) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008.
- (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)," June 2011.