



DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY
REFER
TO:

Joint Interoperability Test Command

8 Feb 13

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Special Interoperability Test Certification of the Sourcefire 3D System Intrusion Protection System and Intrusion Detection System with Software Release 4.10.X

References: (a) DoD CIO, Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," 27 March 2012
(b) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(c) through (f), 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 Sourcefire 3D System Intrusion Protection System (IPS) and Intrusion Detection System (IDS) with Software Release 4.10.X, hereinafter referred to as the System Under Test (SUT), meets all the critical interoperability requirements for an IPS/IDS and is certified for joint use within the Defense Information System Network (DISN). The operational status of the SUT must be verified during deployment. Any new discrepancies that are discovered in the operational environment will be evaluated for impact and adjudicated to the satisfaction of the Defense Information Systems Agency (DISA) via a vendor Plan of Action and Milestones (POA&M) to address the concern(s) within 120 days of identification. JITC conducted testing using IPS/IDS requirements within the Unified Capabilities Requirements (UCR) 2008, Change 3, Reference (c) and IPS/IDS test procedures, Reference (d). JITC does not certify any other configurations, features, or functions, except those cited within this memorandum. This certification expires upon changes that affect IO, but no later than three years from the date of this memorandum.

3. The original certification is based on interoperability testing conducted by the JITC, review of the vendor's Letter of Compliance (LoC), and DISA Information Assurance (IA) Certification Authority (CA) approval of the IA configuration. The JITC conducted interoperability testing at the Indian Head, Maryland test facility from 5 July 2011 through 29 July 2011. The DISA Field Security Operations (FSO), as the DISA CA, has reviewed the IA Findings Report for the SUT, Reference (e), and based on the findings in the report has provided a positive recommendation. JITC issued the original interoperability certification on 1 August 2012. The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation. JITC certifies the SUT has met the UCR requirements for IPS/IDS devices.

JITC Memo, JTG, Extension of the Special Interoperability Test Certification of the Sourcefire 3D System Intrusion Protection System and Intrusion Detection System with Software Release 4.10.X

4. The extension of this certification is based upon Desktop Review (DTR) 1. Sourcefire requested a DTR 1 to install a patch hotfix to close three IA related findings. JITC determined that limited regression testing was required. JITC conducted Verification and Validation testing during 10-14 December 2012 and DTR 1 was successfully verified. The DISA CA concurred with the JITC’s determination and provided a positive recommendation on DTR 1 on 3 January 2013. Therefore, DTR 1 is approved by the JITC and the SUT is now certified for use in the DISN.

5. Section 5.8 of Reference (c) establishes the threshold Capability Requirements/Functional Requirements (CRs/FRs) used to evaluate the interoperability of the SUT as an IPS/IDS. Tables 1 and 2 list the IPS/IDS interfaces, CRs, FRs, and status of the requirements.

Table 1. SUT Interface Interoperability Status

Interface	Critical (See note 1)	UCR Reference (UCR 2008 CH 2)	Threshold CR/FR Requirements (See note 2)	Status	Remarks								
Intrusion Protection System													
10Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces								
100Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces								
1000Base-X	No	5.3.2.4/5.3.3.10.1.2	1-4	Met	SUT met requirements for specified interfaces								
10GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT								
40GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT								
100GBase-X	No	5.3.2.4/5.3.3.10.1.2	1-4	N/A	Not supported by the SUT								
<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. Enclosure 3 of the original Special Interoperability Test Certification provides a list of more detailed requirements for security device products.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Base-X Ethernet generic designation</td> <td style="width: 50%;">GBaseX Gigabit generic designation</td> </tr> <tr> <td>CH Change</td> <td>N/A Not Applicable</td> </tr> <tr> <td>CR Capability Requirement</td> <td>SUT System Under Test</td> </tr> <tr> <td>FR Functional Requirement</td> <td>UCR Unified Capabilities Requirement</td> </tr> </table>						Base-X Ethernet generic designation	GBaseX Gigabit generic designation	CH Change	N/A Not Applicable	CR Capability Requirement	SUT System Under Test	FR Functional Requirement	UCR Unified Capabilities Requirement
Base-X Ethernet generic designation	GBaseX Gigabit generic designation												
CH Change	N/A Not Applicable												
CR Capability Requirement	SUT System Under Test												
FR Functional Requirement	UCR Unified Capabilities Requirement												

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/ Function	Applicability (See note)	UCR Reference (UCR 2008 CH 2)	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																									
	Reserved	N/A	5.8.4.3.2	N/A																									
	Configuration Management	Required	5.8.4.3.3	Met																									
	Alarms & Alerts	Required	5.8.4.3.4	Met	See the Information Assurance Findings and Mitigations Summary Report.																								
	Audit and Logging	Required	5.8.4.3.5	Met	See the Information Assurance Findings and Mitigations Summary Report.																								
	Reserved	N/A	5.8.4.3.6	N/A																									
	Documentation	Required	5.8.4.3.7	Met	See the Information Assurance Findings and Mitigations Summary Report.																								
	Cryptography	Required	5.8.4.3.8	N/A	Cryptography is optional with the exception that all outgoing communications are encrypted.																								
	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	N/A	FW & VPN Only																								
	Filtering	Required	5.8.4.4.2	N/A	FW Only																								
4	IPS Functionality																												
	IPS Security Device Requirements	Required	5.8.4.5	Met	IDS/IPS Only																								
<p>NOTE: Criticality represents high level roll-up of the CR/FR area. Table 3-1 of Enclosure 3 of the original Special Interoperability Test Certification provides detailed CR/FR for each security device product (FW, IPS/IDS, VPN component).</p> <p>LEGEND:</p> <table> <tr> <td>CH</td> <td>Change</td> <td>IP</td> <td>Internet Protocol</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>IPS</td> <td>Intrusion Prevention System</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>N/A</td> <td>Not Applicable</td> </tr> <tr> <td>FW</td> <td>Firewall</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> <tr> <td>IDS</td> <td>Intrusion Detection System</td> <td></td> <td></td> </tr> </table>						CH	Change	IP	Internet Protocol	CR	Capability Requirement	IPS	Intrusion Prevention System	FR	Functional Requirement	N/A	Not Applicable	FW	Firewall	UCR	Unified Capabilities Requirements	ID	Identification	VPN	Virtual Private Network	IDS	Intrusion Detection System		
CH	Change	IP	Internet Protocol																										
CR	Capability Requirement	IPS	Intrusion Prevention System																										
FR	Functional Requirement	N/A	Not Applicable																										
FW	Firewall	UCR	Unified Capabilities Requirements																										
ID	Identification	VPN	Virtual Private Network																										
IDS	Intrusion Detection System																												

6. 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 Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System

JITC Memo, JTG, Extension of the Special Interoperability Test Certification of the Sourcefire 3D System Intrusion Protection System and Intrusion Detection System with Software Release 4.10.X

Tracking Program (STP), 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 Defense Switched Network (DSN) testing is on the Telecommunications Switched Services Interoperability website at <http://jitc.fhu.disa.mil/tssi>. All associated data is available on the DISA Unified Capabilities Certification Office (UCCO) website located at <https://aplits.disa.mil>.

7. JITC testing point of contact is Mr. Keith Watson; commercial (301) 743-4305, e-mail address is Keith.D.Watson2.civ@mail.mil. The JITC certification point of contact is Ms. Baotram (BT) Tran; commercial (301)743-4319, e-mail address is Baotram.Tran.civ@mail.mil. The JITC's mailing address is 3341 Strauss Avenue, Suite 236, Indian Head, Maryland 20640-5149. The UCCO tracking number for the SUT is 1021801.

FOR THE COMMANDER:



for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Enclosures a/s

Distribution (electronic mail):

DoD CIO
Joint Staff J-6, JCS
USD(AT&L)
ISG Secretariat, DISA, JTA
U.S. Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, 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

ADDITIONAL REFERENCES

- (c) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2008, Change 2," December 2010
- (d) Joint Interoperability Test Command, "Security Device Test Plan," June 2011
- (e) Joint Interoperability Test Command, "Information Assurance (IA) Findings Report for Sourcefire 3D Systems Release 4.10.X (Tracking Number 1021801)," April 2012
- (f) Department of Defense Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004