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

IN REPLY REFER TO: Network Services (NSP) 12 May 2014

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) approval of the A10 Networks AX-2000 Series, ASX-3000 Series, and AX-5000 Series Application Delivery Controller (ADC) with Software Release (Rel.) Advanced Core Operating System (ACOS) 2.7.1, Tracking Number (TN) 1230001, as an Information Assurance (IA) Tools (IAT)

Reference: (a) DoDI 8100.04, "DoD Unified Capabilities," 09 Dec 2010
(b) DoD CIO "Unified Capabilities Requirements (UCR) 2013," Jul 2013

1. DoD UC APL approval of the A10 Networks AX-2000 Series (AX2500-010-FIPS), AX-3000 Series (AX3000-11-GCF-FIPS), and AX-5000 Series (AX5200-110-FIPS) ADC Rel. ACOS 2.7.1 TN 1230001 as an IAT has been granted. The Army Chief Information Officer (CIO)/G-6 Certifying Authority (CA) granted IA certification on 23 Aug 2013 based on the security testing completed by the United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC)-led IA test teams. This solution achieved interoperability (IO) certification from the Joint Interoperability Test Command (JITC) on 08 Nov 2013. This approval is effective upon the date of this memorandum and expires **12 Nov 2016** unless a critical issue is identified that invalidates either the IO or the IA posture of this product as determined by the JITC or the CIO for Combatant Commands, Services, and Agencies. Please note that Services and Agencies are required to recertify and reaccredit their systems every three years. Please refer to the UC APL for official posting of this solution at the following URL: https://aplits.disa.mil.

2. This product/solution must be implemented only in the configuration that was tested and approved. When the system is deployed into an operational environment, the following security measures (at a minimum) must be implemented to ensure an acceptable level of risk for the sites' Designated Accrediting Authority (DAA):

a. The site must register the system in the Systems Networks Approval Process (SNAP) Database https://snap.dod.mil/index.cfm as directed by the Defense/IA Security Accreditation Working Group (DSAWG) and the Program Management Office (PMO).

b. The configuration must be in compliance with the A10 Networks AX-2000 Series, ASX-3000 Series, and AX-5000 Series ADC Rel. ACOS 2.7.1 TN 1230001's military-unique features deployment guide.

c. The site must use a Security Technical Implementation Guide (STIG)-compliant Public Key Infrastructure (PKI)-enabled workstation for management of the A10 AX Series ADC. The site may implement the use of a secure token as a two-factor authentication method to mitigate the NET0445 finding, which will be assessed against the A10 AX Series ADC if a secure token is not used. The solution was tested with an A10 demonstration using a Rivest-Shamir-Adelman

(RSA) token. The site can select the secure token of its choice to meet this requirement. If the site is unable to deploy the use of tokens, then the site must implement a defense-in-depth approach for the solution and request the DAA to accept the risk.

d. The site may disable the A10 ADC management web Graphical User Interface (GUI) and use Command Line Interface (CLI) for remote management to mitigate the following findings, which will be accessed against the A10 AX Series ADC if the management web GUI is not disabled: WG140, GEN000400, NET0340, and NET0445.

3. The IO certification letter containing detailed configuration on this product is available at the following URL: http://jitc.fhu.disa.mil/tssi/cert_pdfs/a10_networks_ax_series_adc_nov13.pdf
On 05 May 2014, the following extension was approved via Desktop Review (DTR)#1 (requested to add the Thunder 1030, 3030, 5430 and 6430 Series to the current certification, based on similarity): http://jitc.fhu.disa.mil/tssi/cert_pdfs/a10_ax_series_adc_dtr1_may14.pdf

4. Due to the sensitivity of the information, the Information Assurance Assessment Package (IAAP) that contains the approved configuration and deployment guide for this solution must be requested directly from the Unified Capabilities Certification Office (UCCO) by government civilian or uniformed military personnel.
E-Mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil
UCCO Process Manager: (571) 359-4363

BRITT.EARL.JAMES.JR.1147158781
Digitally signed by BRITT.EARL.JAMES.JR.1147158781
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=BRITT.EARL.JAMES.JR.1147158781
Date: 2014.05.13 14:32:35 -04'00'

For:

JESSIE L. SHOWERS
Chief, DISN and GSM Program
Management Office (NSP)
DISA, Network Services Directorate