



## DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 4502  
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Network Services (NS231)

29 Dec 2010

### MEMORANDUM FOR DISTRIBUTION

**SUBJECT:** Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) approval of the Aruba Networks Wireless Products version 3.3.2.18-FIPS, Tracking Number (TN) 0901301, as Wireless Local Area Network Access System (WLAS) and Wireless Access Bridge (WAB).

Reference: (a) DoDI 8100.3, "DoD Voice Networks," 16 Jan 2004.

1. DoD UC APL approval of the Aruba Networks Wireless Product version 3.3.2.18-FIPS, TN 0901301, as WLAS/WAB has been granted. This solution achieved Information Assurance (IA) Accreditation from the Defense IA/Security Accreditation Working Group (DSAWG) on 05 Oct 2010. This solution achieved Interoperability Certification (IOC) from the Joint Staff (JS) on 08 Dec 2010. This approval is effective upon the date of this memorandum and expires **29 Dec 2013** unless a critical issue is identified that invalidates either the Interoperability or the IA posture of this product as determined by the JS or the Defense Information Systems Network (DISN) Designated Approving Authority (DAA). 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: <http://www.disa.mil/ucco>.

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' 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 DSAWG and the Program Management Office (PMO).
- b. The configuration must be in compliance with the Aruba Networks military-unique features deployment guide.
- c. The system should be incorporated in the site's Public Key Infrastructure (PKI). If PKI is not incorporated, the findings that follow will be included in the site's architecture.
- d. The system should use Remote Authentication Dial-In User Service (RADIUS) or an equivalent device for authentication of wireless users.
- e. The system should use an Lightweight Directory Access Protocol (LDAP) server to authenticate administrator users. RADIUS and Terminal Access Controller Access Control System Plus (TACACS+) authentication of administrative users do not use a FIPS-approved encryption method.
- f. The site should use a SysLog device for auditing purposes.

DISA Memo, NS231, UC APL Approval Memo, Aruba Networks Wireless Products version 3.3.2.18-FIPS, TN 0901301, 29 Dec 2010.

g. As a condition of fielding, the inactivity timer should be configured to control all physical interfaces to the controller, including the serial console port. The timeout should be configured at 5 minutes.

3. The IOC letter containing detailed configuration for this product is available at the following URL: [https://jit.fhu.disa.mil/cert/cert\\_let.11/dec/anwpv33218fips\\_dec10.pdf](https://jit.fhu.disa.mil/cert/cert_let.11/dec/anwpv33218fips_dec10.pdf)

4. Due to the sensitivity of the information, the Information Assurance Assessment Package (IAAP) that contained 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: [ucco@disa.mil](mailto:ucco@disa.mil)

UCCO Process Questions: (520) 538-3234 DSN 879

UCCO Process Manager: (703) 365-8801 ext. 3434

JESSIE L. SHOWERS, JR.  
Chief, Capabilities Center  
DISA, Network Services Directorate