DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Network Services (NS231) 09 Jun 2011

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) approval of Asentria TeleBoss 850 Telecom Site Controller (T850) with Software Release (Rel.) 2.06.230_JTC01 Tracking number (TN) 1013001, as a Customer Premise Equipment (CPE)

Reference: (a) DoDI 8100.04, "DoD Unified Capabilities," 09 Dec 2010.

1. DoD UC APL approval of the Asentria T850 Rel. 2.06.230_JTC01 TN 1013001 as CPE has been granted. This solution achieved Information Assurance (IA) Accreditation from the Defense IA/Security Accreditation Working Group (DSAWG) on 04 Mar 2011. This solution achieved Interoperability Certification (IOC) from the Joint Staff (JS) on 10 May 2011. This approval is effective upon the date of this memorandum and expires **09 Jun 2014** 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 Asentria T850's military-unique features deployment guide.

c. Only two access points will be enabled for management and administration, the serial console port and the Ethernet port used for Secure Shell (SSH) from a site-provided DoD STIG-compliant management workstation.

d. In order to avoid the Internet Control Message Protocol (ICMP) vulnerability, the site must manually configure and document any open ports which correspond with the device(s) sending the Call Data Records (CDRs).

e. TELNET must not be enabled within this solution.

f. Site must use source-IP Address Control List to limit management of the T850.

3. The IOC letter containing detailed configuration on this product is available at the following URL: http://jitc.fhu.disa.mil/tssi/cert_pdfs/asentriat850_may11.pdf

DISA Memo, NS231, UC APL Approval Memo, Asentria T850 Rel. 2.06.230_JTC01 TN 1013001, 09 Jun 2011.

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
UCCO Process Questions: (520) 538-3234 DSN 879
UCCO Process Manager: (703) 365-8801 ext. 3434

SHOWERS.JESSIE.L.JR.1119211235

Digitally signed by SHOWERS.JESSIE.L.JR.1119211235
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=SHOWERS.JESSIE.L.JR.1119211235
Date: 2011.06.11 22:31:08 -04'00'

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