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

IN REPLY REFER TO: Infrastructure Directorate (IE) 18 Sep 2015

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) approval of the Spok (formally Amcom Software, Inc.) Computer Telephony Integration (CTI) Cisco and Avaya Console Workstation Release (Rel.) 5.2-0 Tracking Number (TN) 1214402 as a Customer Premise Equipment (CPE)

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 Spok CTI Cisco and Avaya Console Workstation Rel. 5.2-0 TN 1214402 as a CPE has been granted. The Field Security Operations (FSO) granted Information Assurance (IA) certification on 21 Dec 2012 based on the security testing completed by the Defense Information Systems Agency (DISA)-led IA test teams. This solution achieved Interoperability (IO) certification from the Joint Interoperability Test Command (JITC) on 10 Jan 2013. This approval is effective upon the date of this memorandum and expires **31 Aug 2018** 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 Chief Information Officers (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/apl.

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 Spok CTI Cisco and Avaya Smart Console Workstation Rel. 5.2-0 TN 1214402's military-unique features deployment guide.

c. The system must be incorporated in the site's Public Key Infrastructure (PKI). If PKI is not incorporated, the following findings will be included in the site's architecture:

- DSN13.17 for Amcomdb and Amcomsb
- DSN 18.10 for Amcomdb and Amcomsb
- NET0445 for Amcomdb and Amcomsb

d. The system must be integrated into the site's Active Directory (AD) environment for authentication and authorization requirements.

e. The system must use a Remote Authentication Dial-In User Service (RADIUS) or equivalent device for authentication.

f. The site must use a SysLog device for auditing purposes.

g. If access to the database on the Amcomsb server is not manage using the Public Key (PK)-enabled Secure Shell (SSH) client, the following finding will be included in the site's architecture: DG0065 for Amcomdb.

h. If remote access is not implemented in the secure manner described within the Oracle 9-11 Database Security Technical Implementation Guide (STIG) Checklist, the following finding will be included in the site's architecture: DG0186 for Amcomdb and Amcomsb.

i. The site must deploy the Amcomdb and Amcomsb on physically separated servers. If the components are not deployed in this manner, the following finding will be included in the site's architecture: WG204 for Amcomdb and Amcomsb.

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/amcom_cti_cisco_avaya_scw_4_90_jan13.pdf
On 07 Feb 2014, the following extension was approved via Desktop Review (DTR) #1 (to update the software from Rel. 4.9-0 to 5.2-0, which only included fixes for the IA Plan of Action and Milestones (POA&Ms): http://jitc.fhu.disa.mil/tssi/cert_pdfs/amcom_cti_cisco_avaya_r5_2-0_dtr1_feb14.pdf
On 31 Aug 2015, the following extension was approved via DTR #2 (requested to extend this solution's listing on the UC APL by an additional 3 years):
http://jitc.fhu.disa.mil/tssi/cert_pdfs/Spok_AMCOM_CTI_Cisco_Avaya_TN1214402_DTR2_Sep15.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.ie.list.unified-capabilities-certification-office@mail.mil

GRADIJAN.ROBERT.GEORGE.1398029980
Digitally signed by GRADIJAN.ROBERT.GEORGE.1398029980
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=GRADIJAN.ROBERT.GEORGE.1398029980
Date: 2015.09.21 09:58:53 -04'00'

For:

JESSIE L. SHOWERS, JR.
Infrastructure Executive