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

IN REPLY REFER TO: Network Services (NSP) 07 Aug 2014

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) approval of the LiteScape Biometric Secure Profile Authentication Reader (SPAR)™ with Firmware Version 3.0 and Secure Profile Management (SPM) Release (Rel.) 4.4 Tracking Number (TN) 1015201 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 LiteScape Biometric SPAR™ with Firmware Version 3.0 and SPM Rel. 4.4 TN 1015201 as a CPE has been granted. The Field Security Operations (FSO) granted Information Assurance (IA) certification on 19 Jul 2011 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 Staff (JS) on 09 Aug 2011. This approval is effective upon the date of this memorandum and expires **07 Aug 2017** 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.

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 LiteScape Biometric SPAR™ with Firmware Version 3.0 and SPM Rel. 4.4 TN 1015201'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:

- APP3280 for LiteScape SPM 1.00.0000 (LiteScape SPM1 and SPM2)
- DSN13.17 for LiteScape SPM1 and LiteScape SPM2
- NET0445 for LiteScape SPM1 and LiteScape SPM2
- WG140 for LiteScape SPM1 and LiteScape SPM2
- WG145 for LiteScape SPM1 and LiteScape SPM2
- WG350 for LiteScape SPM1 and LiteScape SPM2

DISA Memo, NSP, UC APL Approval Memo, LiteScape Biometric SPAR™ with Firmware Version 3.0 and SPM Rel. 4.4 TN 1015201, 07 Aug 2014.

- WG350 for LiteScape SPM1 and LiteScape SPM2

d. There will be no administrator access for identification or authentication to the database. All management must be done through the LiteScape SPM Web interface. The database is used in the background to work with the application and does not require an administrator to manage it. If not followed the following finding will be included in the site's architecture: DG0065

e. The site must use a Host-Based Intrusion Detection System (HIDS).

f. The site must use CUCM Secure Sockets Layer (SSL) certificates in order for the SPAR to be compliant.

g. Trivial File Transfer Protocol (TFTP) must only be used for upgrading the SPAR firmware.

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/litescapebiometricspm_tn1015201.pdf
On 07 Aug 2014, the following extension was approved via Desktop Review (DTR) #1 (requested to extend this solution's listing on the UC APL by 3 years)

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: 2014.08.07 15:00:20 -04'00'

For:

JESSIE L. SHOWERS, JR., PMP
Vice Director for Network Services