DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MATERIEL COMMAND
9301 CHAPEK ROAD
FORT BELVOIR, VA 22060-5527

REPLY TO ATTENTION OF:

CPM 25-15
Expires: 5 February 2012

AMCIO-FTM

5 February 2010

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum - Acceptance of Risk Letter (ARL) to use Odyssey Access Clients compatible with VISTA and Windows Mobile/CE for wireless devices on AMC Depot Switched Architecture Wireless LANs (SAWLAN).

1. I authorize the use of the Odyssey Access Clients (FIPS Edition 4.57 and 5.1) to provide a secure wireless connection for devices in the AMC Enterprise Network for the following period 1 January 2010 to 1 June 2011.

2. The current supplicants do not support the mandated VISTA operating system, or the requirements for the handheld terminals currently in use for a significant portion of our depot operating environment.

3. Point of contact for this action is the AMC G6, Core Technologies Division, AMCIO-FT, DSN 656-8563 or 703-806-8563.

FOR THE COMMANDER:

EDWARDS.TERENCE.M.1205184690
Digitally signed by EDWARDS.TERENCE.M.1205184690
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=EDWARDS.TERENCE.M.1205184690
Date: 2010.02.05 10:10:09 -05'00'

Encl

TERENCE M. EDWARDS
Chief Information Officer/G6

DISTRIBUTION:
B
H

Background

1. The Army has mandated that all Windows-based computers migrate to Microsoft's Vista OS NLT Dec. 31, 2009. This creates a problem because there is not an approved SIP Client on the Army Information Assurance Approved Products List (AIAAPL) that will support VISTA at this time. A waiver to continue the use of Windows XP or an Acceptance of Risk Letter (ARL) from the Designated Approval Authority (DAA) will be necessary to allow the use the appropriate client.

2. U.S. Army Materiel Command's (AMC) Special Installation Depots have deployed the Microsoft VISTA solution for industrial based operations across the enterprise and do not have an authorized access client to encrypt these sessions. In addition, handheld terminals currently being fielded require the advanced software now currently being validated by the Army.

3. Vendors are aggressively working with the Technology Integration Center (TIC) and Office of Information Assurance and Compliance (OIA&C) for security validation of Odyssey Access Client (OAC) Federal Information Processing Standards (FIPS) Edition clients.

4. Mr. Edwards is the DAA for AMC and has authorized the use of the VISTA and Windows Mobile/CE clients (OAC FIPS Edition 5.1 and OAC FIPS Edition 4.57). The following criteria have been considered to determine the potential risk acceptable:

a. Although the new versions have not been through the validation process for the TIC, Joint Interoperability Test Command (JITC), or a Certificate of Networthiness (CON), they are based on the same cryptographic library used for the previously Army approved OAC version.

b. Retina – Network Security Scanner was used to examine any potential security vulnerabilities by the Anniston Army Depot DOIM. A localized computer using the Vista OS running the Juniper OAC were tested. No vulnerabilities were indicated.

c. Proposed OAC conforms to FIPS guidelines, using EAP-TLS authentication, 802.11i (WPA2) key derivation, and AES-CCMP data encryption.

d. Has been accepted into evaluation for conformance to the Common Criteria (ISO/IEC 15408).

e. Is compatible with U.S. Department of Defense Common Access Card (CAC) standards and certificates.

f. Supports the xSec protocol, using 256-bit Advanced Encryption Standard (AES) and Layer 2 header encryption.

g. AMC locations are currently using the newer OAC FIPS-Edition software to support mission activity due to the requirement to operate in a Vista OS environment.

5. Authorized approval for FIPS Edition OAC includes:

a. OAC FIPS Edition version 4.57 for handheld devices uses Odyssey Security Component (OSC) 1.2, which has the National Institute of Standards and Technology (NIST) certificate #569. OSC 1.2 is supported on Windows XP, Windows 2000, Windows Mobile 5 & 6, and Windows CE 5.

b. OAC FIPS Edition 5.1 uses OSC 2.0, which has the NIST certificate #1189. OSC 2.0 is currently supported on Windows XP, Windows Vista, and Windows 2000.

6. Point of contact for this action is the AMC G6, Core Technologies Division, AMCIO-FT, DSN 656-8563 or 703-806-8563.