ADDENDUM TO APPENDIX A, THE LMP TAV-C PORTAL END USER ACCESS PROCEDURES AND AMC OPORD, FRAGO 2, 19-220

To avoid excessive contract modification costs, it was decided in the development of Total Asset Visibility-Contractor (TAV-C) capability in LMP to require all new relevant contracts or new orders to it to be used rather than modify existing contracts. In a step to make participation in Army support more attractive, the decision was made to use the DoD approved External Certification Authority (ECA) certification in lieu of a full security clearance for TAV-C portal users.

TAV-C completed development and post go-live support period on 23 June 2020 with no contracts being processed. The first contracts are now beginning to be finalized and a problem as been found.

Problem.

Procedures developed for contractors' access requests mirrored those for Army employees. As currently written, the applications require IA training, a signed Acceptable Use Policy (AUP) statement, and the ECA certificate to be provided with a DD Form 2875 System Authorization Access Request (SAAR). It has been determined the use of the SAAR form is not applicable since the ECA certificate process does not require a security clearance so there is no entry in JPAS for a security manager to validate.

Upon further review, G-2/6 determined the ECA certificate was sufficient for portal users, but the use of the SAAR is inappropriate for requests from ECA certified individuals. In order to have an auditable user access process to LMP, it will be necessary to still have a standard account access process across AMC.

Remediation.

Contractor Responsibility. The application packet shall consist of the 1) user's ECA form, 2) Memorandum for Record on company letterhead paper signed by the contractor Security Manager or an individual with Company Equity Ownership attesting that all documentation needed to complete the ECA Digital Certificate Forms Packet was witnessed at the time of Notarization. 3) completion of cyber security training as evidenced by copy of training certificate. 4) signed AUP. An electronic copy of all the documents listed in this section shall be provided to the appropriate Government Point of Contact before LMP access can be granted.

The applicant can take the cyber security training at (https://public.cyber.mil/training/.

A blank AUP will be provided and can be manually signed and scanned..

LCMC Responsibility. Appoint a government POC for LMP access and oversight. To ensure validity over time, the requiring activity will evaluate the efficacy of the contractor's TAV-C portal access control procedures for effectiveness, accuracy and the upkeep of their TAV-C access files. Maintain records of certificates accepted and their expiration date and establish procedures to ensure certificates are maintained as current and valid by the contractor.

AMC DCS G3, Supply Requirements Division is publishing this memorandum as an addendum to the LMP TAV-C Portal User Access Procedures and FRAGO 2, AMC OPORD 19-229 to provide interim guidance until revisions to the user's guide and other related documents to the established solution can be accomplished per recommendations by the G-2/6 within the LCMC and ACC activities processing these contracts. This addendum can be used to enable the completion of pending contracts before year-end and will remain in effect until next release of the portal user access guide. Please insert a copy of this addendum in to the user’s guide.

10/15/2020

X Daniel C. Parker, PhD

DR. DANIEL C. PARKER
Chief, AMC G3 Supply Requirements Division
Signed by: PARKER.DANIEL.C.1171814622