PCS JTF Personal Property Advisory #26-0025B

Date: 26 January 2026

From: Permanent Change of Station Joint Task Force (PCS JTF), Defense Personal Property Management Office (DPMO), Scott AFB, IL 62225

To: All Military Service Headquarters Representatives, Worldwide Personal Property Shipping Offices (PPSOs), Personal Property Processing Offices (PPPOs), and Approved Department of War (DoW) Personal Property Transportation Service Providers (TSPs)

Subject: Defense Personal Property Cybersecurity Maturity Model Certification (CMMC) Implementation Plan Update – CMMC Unique Identifier (UID) Requirement

Revisions within this document are highlighted in red text.

1. Situation: TSPs routinely handle DoW customers' Personally Identifiable Information (PII), which is categorized as Controlled Unclassified Information (CUI), during day-to-day Defense Personal Property Program (DP3) Tender of Service (ToS) activities.

2. General Cybersecurity Requirements: To protect CUI and Federal Contract Information (FCI) created used in the ToS, the Government is implementing a phased approach toward increasing cybersecurity controls. This phased approach is modeled on the DoW's Cyber Maturity Model Certification (CMMC), which began implementation on 10 November 2025.

a. ToS Phase 1: By 15 March 2026, TSPs and subcontractors will complete an affirmation of continuous compliance with CMMC Level 1 assessment requirements in the Supplier Performance Risk System (SPRS) (https://piee.eb.mil) applicable to each of the TSP information technology systems that process, store, or transmit FCI or CUI and that are used in performance of the ToS. **TSP affirmation is required to be awarded any shipments on or after 15 May 2026**.

b. ToS Phase 2: By 15 March 2027, TSPs and subcontractors will complete an affirmation of continuous compliance with CMMC Level 2 assessment requirements in SPRS applicable to each of the TSP information systems that process, store, or transmit FCI or CUI and that are used in performance of the ToS. **TSP affirmation is required to be awarded any shipments on or after 15 May 2027**.

c. Subcontractor Compliance: TSPs are required to ensure their subcontractor network and suppliers complete an affirmation of continuous compliance with the requirements applicable to the CMMC level required for the subcontract or other contractual instrument for each of the subcontractor information technology systems that process, store, or transmit FCI or CUI and that are used in performance of the subcontract.

d. All TSPs are required to provide the CMMC UID used for CMMC affirmation in SPRS to the DPMO at transcom.scott.tcj9.mbx.pp-quals@mail.mil NLT 15 Mar 2026. These UIDs are crucial for the purpose of validating the completions of CMMC assessments by TSPs in SPRS. CMMC UIDs are assigned by SPRS.

3. Cybersecurity Incident Reporting: "Cyber Incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information technology system and/or the information residing therein.

a. Reportable cyber incidents (regardless of whether the information technology system contains FCI or CUI or there is an impact to performance such as delivery schedule delay), include, but are not limited to, the following:

(1) Root Level Intrusion, User Level Intrusion, Denial of Service, Malicious Logic, and Ransomware.

(2) Notifications by a federal, state, or local law enforcement agency or cyber center (i.e., National Cyber Investigative Joint Task Force (NCIJTF), National Cybersecurity & Communications Integration Center (NCCIC)) of being a victim of a successful or unsuccessful cyber-event, anomaly, incident, insider threat, breach, intrusion, or exfiltration.

b. When a cyber incident occurs,

(1) The contractor is required to notify USTRANSCOM Cyber Operations Center (CyOC) as soon as practical, but no later than 72 hours after discovering a reportable cyber incident. The reporting timeline begins when the incident is discovered or reported to the company, its employees, contractors, or cybersecurity firm responsible for providing cybersecurity and response for the company. The USTRANSCOM Cyber Operations Center (CyOC) via phone at 618-817-4222. If the TSP does not immediately reach the CyOC via phone, the TSP shall send an email notification to transcom.scott.tcj6.mbx.cyoc-dodin- operations@mail.mil.

(2) The TSP shall provide a follow-on cyber incident report to the USTRANSCOM CyOC within five calendar days of becoming aware of a reportable cyber-incident.

(3) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

4. Full details are listed in the attached document, are incorporated into the 2026 DP3 Tender of Service business rules. Note that this attachment corrects a substantive typo that was included in the original attachment to PCS JTF Personal Property Advisory #26-0025.

5. Government assistance can be obtained from the following resources:

a. USTRANSCOM TCJ6 Cyber Analysis & Engagement Branch: scott.tcj6.mbx.xa@mail.mil

b. DoD–Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE): https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/

c. NSA Central Security Service/DIB Cybersecurity Services: https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/#:~:text=Contractor%20Protection&text=Once%20you%20sign%20a%20contract,to%20non%2Dpublic%20DoD%20information

d. Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

e. Defense Criminal Investigation Services Cyber Field Office: https://www.dodig.mil/Portals/48/Documents/Components/DCIS/Poster%20and%20Brochures/DCIS_CyberCrime.pdf?ver=2017-03-24-162427-917

f. DoW Chief Information Officer: https://dodcio.defense.gov/CMMC/

6. This message was approved for release by the Chief of Operations, PCS JTF Defense Personal Property Management Office.

Attachment: 2025.10.03 DPMO ToS Cyber Language v1.1