SUBPART 4.73 —SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

(Revised April 30, 2021 through PROCLTR 2021-10)

Parent topic: PART 4 – ADMINISTRATIVE MATTERS

4.7301 Definitions.

See 2.101 for definitions of “collaboration folders,” “DLA Export Control Technical Data Access,” “enhanced validation,” and “JCP Certification.” See DFARS 204.7301 for definitions of “controlled technical information” and “covered defense information.” See DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, paragraph (a) for definitions of “covered defense information,” “operationally critical support,” and “cyber incident.” See DoDD 5230.25, Withholding of Unclassified Technical Data From Public Disclosure, E2.1.2 for definition of “critical technology.”

4.7303-1 General.

Contracting officers shall follow the guidance at DFARS PGI 204.7303-1(a) and (b), Safeguarding Covered Defense Information and Cyber Incident Reporting, Procedures, General.

(a) In addition to the requirements at DFARS PGI 204.7303-1(a):

(1) For services and items without a material master that require access to controlled technical data or information**,** the requiring activity will provide a performance work statement (PWS) or performance specification that identifies the need for contractors to access covered defense information (CDI). Contracting officers shall review the PWS or performance specification and associated data that the requiring activity determined contains, utilizes, or may result in the generation of CDI and conditions that may potentially arise after award that may result in the generation of CDI to confirm the requiring activity identified the need for contractors to access CDI.

(2) For NSN and LSN items that require access to controlled technical data or information, the product specialist will update the Purchase Order Text (POT) to include Standard Text Objects (STOs) RD002, Covered Defense Information Applies, or RD003, Covered Defense Information Potentially Applies; and RQ032, Export Control of Technical Data (see 25.7901-4(S-90). These STOs constitute notice to contracting officers that the requiring activity expects the solicitation to result in a contract, task order, or delivery order that will involve controlled technical information.

(b) DLA may require additional contractor qualifications to access controlled technical information. For export-controlled items, see subpart SUBPART 25.79 – EXPORT CONTROL.

(S-90) The requiring activity may be internal to DLA or external. Contracting officers should coordinate with the supply planner or other customer-facing personnel to identify the requiring

activity, if unknown. Contracting officers should collaborate with the requiring activity to identify covered defense information and/or operationally critical support.

4.7303-3 Cyber incident and compromise reporting.

(a)(S-91) If the contracting officer receives notice from the DoD Cyber Crime Center (DC3) and DLA is the requiring activity—

(i) Following receipt of the DC3 ICF notification of a cyber incident, the DLA requiring activity will—

(A) Communicate directly only with the contracting officer regarding the incident. The contracting officer is the only individual responsible for all direct communications with the contractor regarding the cyber incident;

(B) Submit a Special Situation Report (Special SITREP) in accordance with instructions and template at DLA DTM 17-017, Commander's Critical Information Requirements (CCIR) Reporting Policy Changes (https://dlamil.dps.mil/sites/InfoOps/CCIR/Forms/AllItems.aspx); and

(C) Contact the Damage Assessment Management Office (DAMO) (OSD Liaison Telephone (410) 694-4380), and request point of contact information if the DAMO has not already initiated contact;

(D) Coordinate with the DAMO to decide whether to submit a request for contractor media in accordance with the clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, paragraph (e); and provide notice of the decision with supporting rationale to the contracting officer; and

(E) Assess and implement appropriate programmatic, technical, and operational actions to mitigate risks identified in the damage assessment report and update the Program Protection Plan to reflect any changes resulting from the assessment.

(ii) The DLA Information Operations Cyber Security Team Manager/System Security Engineer, J61, will—

(A) Provide support to the DLA requiring activity by assisting in the assessment of risk and mitigation strategy associated with the cyber incident; and

(B) If the requiring activity requests an assessment of contractor compliance with the requirements of DFARS 252.204-7012, consult with the contracting officer before beginning the assessment.

(S-92) If the contracting officer receives notice from the DC3 and the requiring activity is external to DLA, the contracting officer shall—

(i) Submit the Special SITREP (see 4.7303-34.7303-3 Cyber incident and compromise reporting. (a)(S-91)4.7303-3 Cyber incident and compromise reporting. (i)4.7303-3 Cyber incident and compromise reporting. (B)4.7303-3 Cyber incident and compromise reporting.)); and

(ii) Provide the DC3 notice to the DLA Cyber Emergency Response Team (CERT) (cert@dla.mil).