<?xml encoding="UTF-8">

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.

Parent topic: SUBPART 4.73 —SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING