PART 4 – ADMINISTRATIVE MATTERS

(Revised January 15, 2021 through PROCLTR 2021-03)

TABLE OF CONTENTS

SUBPART 4.2 – CONTRACT DISTRIBUTION

(Revised September 9, 2016 through PROCLTR 2016-09)

4.270 Electronic Document Access.

4.270-2 Procedures.

(a)(2) Contracting officers will accept or reject contract deficiency reports (CDRs) in EDA within 10 days of submission, and resolve the CDR within 30 days of submission. The DLA Acquisition Operations Division is responsible to track and report performance on a monthly basis to the SPE. Procuring organizations shall track and report monthly to the HCA.

SUBPART 4.5 – ELECTRONIC COMMERCE IN CONTRACTING

(Revised June 11, 2020 through PROCLTR 2020-12)

4.502 Policy.

(b) The DLA Internet Bid Board System (DIBBS) (https://www.dibbs.bsm.dla.mil/) is the DLA supplier-facing portal utilized to:

(i) Post solicitations, solicitation amendments, awards, and award modifications;

(ii) Facilitate submission of quotations by suppliers in response to request for quotations;

(iii) Enable upload of offers in response to request for proposals;

(iv) Convey important messages to the supplier community; and

(v) Transmit notices of proposed contract actions and awards to the GPE/FedBizOpps.

Contracting officers shall include procurement note L01 in DIBBS solicitations for purchase orders and contracts (except indefinite delivery/indefinite quantity task or delivery order contracts, requirements contracts, and multiple award federal supply schedule-type contracts).

*****

L01 Electronic Award Transmission (JUN 2020)

DLA provides notice of awards by either—

(1) Electronic email containing a link to the electronic copy of the Department of Defense (DD)

Form 1155, Order for Supplies or Services, on the DLA Internet Bid Board System (DIBBS); or

(2) Electronic Data Interchange (EDI) 850 utilizing American National Standards Institute (ANSI) X12 Standards through a value added network (VAN) approved by DLA Transaction Services.

Offerors/contractors can obtain information regarding EDI, ANSI X12 transactions, and VANs approved by DLA Transaction Services at Defense Automatic Addressing System (DAAS) Value Added Network List (https://www.transactionservices.dla.mil/daashome/edi-vanlist-dla.asp).

Offerors should direct questions concerning electronic ordering to the appropriate procuring organization point of contact below:

DLA Land and Maritime, Helpdesk.EBS.L&M.LTCs@dla.mil

DLA Troop Support, dlaedigroup@dla.mil

*****

Contracting officers shall include procurement note L02 in DIBBS solicitations for indefinite-delivery/indefinite quantity task or delivery order contracts, requirements contracts, and multiple award federal supply schedule-type contracts.

*****

L02 Electronic Order Transmission (JUN 2020)

Offerors shall select one of the following alternatives for paperless order transmission:

( ) American National Standards Institute (ANSI) X12 Standards through a value added network (VAN) approved by DLA Transaction Services; or

( ) Electronic mail (email) award notifications containing web links to electronic copies of the Department of Defense (DD) Form 1155, Order for Supplies or Services.

Offerors must register on the DLA Internet Bid Board System (DIBBS) (https://www.dibbs.bsm.dla.mil/) to receive email notification.

If the offeror elects ANSI/VAN order transmission, DLA will send Electronic Data Interchange (EDI) transaction sets at time of award. The contractor shall acknowledge receipt of transaction sets with a functional acknowledgement or order receipt message within 24 hours. If the contractor receives the award transaction set on a weekend or Federal holiday, the contractor shall acknowledge receipt on the next business day. This acknowledgement will confirm that the contractor’s interface with the system is working as needed for contract ordering.

Offerors can obtain information regarding EDI, ANSI X12 transactions, and VANs approved by DLA Transaction Services at Defense Automatic Addressing System (DAAS) Value Added Network List (https://www.transactionservices.dla.mil/daashome/edi-vanlist-dla.asp).

Offerors should direct questions concerning electronic ordering to the appropriate procuring organization point of contact below:

DLA Land and Maritime, Helpdesk.EBS.L&M.LTCs@dla.mil

DLA Troop Support, dlaedigroup@dla.mil

DLA Aviation, avnprocsysproceddiv@dla.mil, phone # 804-279-4026

*****

SUBPART 4.6 – CONTRACTING REPORTING

(Added October 13, 2020 in accordance with PROCLTR 2020-23)

4.606 Reporting Data.

4.606-90 Source selection process data element.

(a) In accordance with (DPC) Memorandum **Reporting Source Selection Process in Federal Procurement Data System (FPDS)** (https://www.acq.osd.mil/dpap/policy/policyvault/USA000991-20-DPC.pdf), dated May 21, 2020, contracting officers shall report the Source Selection Process data element in FPDS using one of the following codes, unless an exception at 4.606-90(b) applies:

CODES FOR REPORTING "SOURCE SELECTION PROCESS" IN FPDS

Code	Short Description	Long Description
LPTA	Lowest Price Technically Acceptable	Select this option if contract award used the LPTA source selection process. LPTA is defined in FAR subpart 15.101-2, but select this option if the process was used for competitive procurements conducted in accordance with other subparts (e.g., 8, 12, 13, 16).
TO	Trade-off	Select this option if contract award used any type of best value trade-off process using price/cost and nonprice/cost factors to determine the successful offeror award. Trade-off is defined in FAR subpart 15.101-1, but select this option if the process was used for competitive procurements conducted in accordance with other subparts (e.g., 8, 12, 13, 16).
O	Other	Select this option if contract award did not use LPTA or a Trade-off process to determine the successful offeror (e.g., price-only, sole-source).

(b) The Source Selection Process data element is not a required data field for blanket purchase agreements (BPAs) issued using part 13 procedures; task and delivery orders issued using single-award indefinite-delivery contracts; and call orders issued under single-award BPAs and using FAR part 8 procedures.

(c) Contracting officers shall not leave the Source Selection Process data field blank.

(d) Contracting officers shall enter—

(1) O for non-competitive awards.

(2) One of the choices in the table at 4.606-90(a) for competitive awards.

(3) LPTA or TO when the contracting officer used a source selection process on awards issued using FAR section 15.101.

(4) O for fully automated actions. In accordance with the DLA Master Solicitation for Automated Simplified Acquisitions, the program evaluates all qualified quotations based on price alone and does

not consider quantity price breaks.

(5) TO for automated requirements that are evaluated and awarded manually. In accordance with the DLA Master Solicitation for Automated Simplified Acquisitions, manual evaluation factors include price, delivery, and past performance in accordance with the terms in the solicitation.

(6) The code consistent with the evaluation procedures cited in the RFQ/RFP for all manually solicited requirements, even if only one offeror responded.

(7) TO for all manual solicitations that may include language for a potential best value trade-off (e.g. use of past performance).

SUBPART 4.7 - CONTRACTOR RECORDS RETENTION

(Revised June 11, 2020 through PROCLTR 2020-12)

4.703 Policy.

(a) Contracting officers shall include procurement note C03 in solicitations and awards.

*****

C03 Contractor Retention of Supply Chain Traceability Documentation (JUN 2020)

(1) By submitting a quotation or offer, the contractor, if it is not the manufacturer of the item, is confirming it currently has, or will obtain before delivery, and shall retain documented evidence (supply chain traceability documentation), as described in paragraph (2) of this procurement note, demonstrating the item is from the approved manufacturer and conforms to the technical requirements.

(2) At a minimum, the supply chain traceability documentation for the item shall include: basic item description, part number and/or national stock number, manufacturing source, manufacturing source's Commercial and Government Entity (CAGE) code, and clear identification of the name and location of all supply chain intermediaries between the manufacturer to the contractor to item(s) acceptance by the Government. The documentation should also include, if available, the manufacturer's batch identification for the item(s), such as date codes, lot codes, or serial numbers.

(3) Contractors can find examples of acceptable supply chain traceability documentation at the Counterfeit Detection and Avoidance Program (CDAP) Website (http://www.dla.mil/LandandMaritime/Business/Selling/Counterfeit-Detection-Avoidance-Program/).

(4) The contractor shall immediately make documentation available to the contracting officer upon request. The contracting officer determines the acceptability and sufficiency of documentation. The contractor shall retain supply chain traceability documentation for six years after final payment under this contract for audit and other valid government purposes. If the contractor fails to retain or provide the documentation, or the contracting officer finds the documentation to be unacceptable, the contracting officer may take corrective action, including, but not limited to, cancellation of undelivered orders or rejection of delivered supplies.

*****

SUBPART 4.8 – GOVERNMENT CONTRACT FILES

(Revised May 10, 2019 through PROCLTR 2019-11)

4.802 Contract files.

(f) DLR sites shall follow the processes and systems at the Military Services sites.

4.804 Closeout of contract files.

Contracting officers shall follow the FAR standard timeframe for closeout. Contracting officers shall assess the validity of their unliquidated obligations (ULOs) that are 120 calendar days or more past the contract delivery date in accordance with DLAM 7010.02, Unliquidated Obligations (ULO) and Undelivered Orders (UDO) Management (https://issue-p.dla.mil/Published_Issuances/Unliquidated Obligations (ULO) and Undelivered Orders (UDO) Management.pdf).

4.805 Storage, handling, and contract files.

(a) Procuring organizations shall follow the Records Management Procurement Job Aid for storage and retrieval of electronic documents.

(1) Procuring organizations shall store all acquisition contract file records in EProcurement "Records Management," the official DLA records repository, except as stated in 4.805(b).

(2) Procuring organizations shall upload to Records Management all obligations documents (e.g. contract awards; and modifications affecting the overall contract obligation, such as those for equitable adjustments or raising the contract ceiling), to include bilateral signature pages. Follow the procedures for saving and naming conventions in the Procurement Job Aid entitled Completing Forms in Document Builder (https://dlamil.dps.mil/:w:/r/sites/InfoOps/_layouts/15/doc2.aspx?sourcedoc=%7B950AD3EC-CE42-444C-B2E6-1A3BB848637A%7D&file=Completing Forms in Document Builder -15 Feb 19.doc&action=default&mobileredirect=true).

(3) When a condition at 4.805(b) applies, include a reference statement in the Records Management contract file notifying authorized users of the location of any document or material maintained outside Records Management.

(b) Procuring organizations shall maintain contents of contract files outside EProcurement Records Management in accordance with the following:

(1) Maintain documents containing personally identifiable information (PII), legal reviews, documents marked as contractor proprietary information, and oversized or voluminous documents as a hard copies or in an electronic, restricted-access location (e.g., eWorkplace Sharepoint site or local share drive).

(2) Maintain classified documents in hard copy only.

(3) Maintain material that cannot be converted to electronic format (e.g., samples, models) in a secured, restricted-access location.

(4) Maintain contractor bid or proposal information or any other source selection

information not marked proprietary as hard copies or in an electronic, restricted-access location until time of award. After award, procuring organizations may upload the documents into Records Management or maintain them in an electronic, restricted-access location. Procuring organizations may maintain oversized or voluminous documents as hard copies.

(c) HCAs shall ensure compliance with this policy.

(S-90) Retain Financial Management Regulation records for 10 years in accordance with DLA Finance Director memorandum dated September 15, 2016, SUBJECT: New DoD Change for Financial Record Retention in Support of Audit Compliance. This policy applies only to records necessary to support financial transactions and financial statement balances; and document evidence of effective internal controls over financial reporting (e.g., reviews and approvals).

SUBPART 4.13 – PERSONAL IDENTITY VERIFICATION

(Revised January 15, 2021 through PROCLTR 2021-03)

4.1302 Acquisition of approved products and services for personal identity verification.

(c) DLA Information Operations is responsible for determining compliance.

4.1303 Contract clause.

4.1303-90 Personal identity verification of contractor personnel.

The contracting officer shall insert procurement note H14, Contractor Personnel Security Requirements, in solicitations and contracts that contain FAR 52.204-9, Personal Identity Verification of Contractor Personnel, when contract performance requires contractor access to Federally controlled facility and/or access to a Federally controlled information system. Contractors requiring intermittent access for a period of less than six months shall obtain approval from the installation security office through the contracting officer.When the contractor employee(s) is/are required to obtain a Common Access Card (CAC) and DLA will serve as the Trusted Agent, follow the procedures in DLA SOP J72.001, Contractor Common Access Card (CAC) Issuance and Accountability Process for DLA Contracts (https://dlamil.dps.mil/sites/Acquisition/Shared Documents/CONTRACTOR CAC SOP J72.001.pdf).

For all contracts where contractor CACs and/or Installation Access Badges will be issued, contracting officers shall ensure that responsibilities for oversight and retrieval of contractor CACs and Installation Access Badges are addressed in the COR designation letter. If a COR is not designated, the contracting officer is responsible for oversight and retrieval of contractor CACs and Installation Access Badges issued under the contract.

If contract performance is to occur at a non-DLA site and the site has physical site and/or information technology security requirements, in addition to the DLA CAC requirements, the contracting officer shall identify those requirements and include them in the solicitation and subsequent contract.

*****

H14 Contractor Personnel Security Requirements (JAN 2021)

(a) Work to be performed under this contract or task order may, in full or in part, be performed at the Defense Logistics Agency (DLA) Headquarters (HQ), DLA field activity office(s), or other Federally-controlled facilities. Prior to beginning work on a contract, DLA requires all contractor personnel working on the Federally-controlled facility to have, at a minimum, an initiated National Agency Check with Written Inquiries (NACI) or NACI equivalent and favorable completion of a Federal Bureau of Investigation (FBI) fingerprint check.

(b) Additionally, in accordance with Department of Defense (DoD) Regulation 5200.2-R, Personnel Security Programs, and DLA Issuance 4314, Personnel Security Program, all DoD contractor personnel who have access to Federally-controlled information systems must be assigned to positions which are designated at one of three information technology (IT) levels, each requiring a certain level of investigation and clearance, as follows:

(1) IT-I for an IT position requiring a single scope background investigation (SSBI) or SSBI equivalent;

(2) IT-II for an IT position requiring a National Agency check with Law and Credit (NACLC) or NACLC equivalent; and

(3) IT-III for an IT position requiring a NACI or equivalent.

Note: IT levels will be designated according to the criteria in DoD 5200.2-R.

(c) Previously completed security investigations may be accepted by the Government in lieu of new investigations if determined by the DLA Intelligence Personnel Security Office to be essentially equivalent in scope to the contract requirements. The length of time elapsed since the previous investigation will also be considered in determining whether a new investigation is warranted. To assist the Government in making this determination, the contractor must provide the following information to the respective DLA Intelligence Personnel Security Office immediately upon receipt of the contract. This information must be provided for each contractor employee who will perform work on a Federally-controlled facility and/or will require access to Federally-controlled information systems:

(1) Full name, with middle name, as applicable, with social security number;

(2) Citizenship status with date and place of birth;

(3) Proof of the individual’s favorably adjudicated background investigation or NACI, consisting of identification of the type of investigation performed, date of the favorable adjudication, name of the agency that made the favorable adjudication, and name of the agency that performed the investigation;

(4) Company name, address, phone and fax numbers with email address;

(5) Location of on-site workstation or phone number if off-site (if known by the time of award); and

(6) Delivery order or contract number and expiration date; and name of the contracting officer.

(d) The contracting officer will ensure that the contractor is notified as soon as a determination is made by the assigned or cognizant DLA Intelligence Personnel Security Office regarding acceptance of the previous investigation and clearance level.

(1) If a new investigation is deemed necessary, the contractor and contracting officer will be

notified by the respective DLA Personnel Security Office after appropriate checks in DoD databases have been made.

(2) If the contractor employee requires access to classified information and currently does not have the appropriate clearance level and/or an active security clearance, the DLA Intelligence Personnel Security Office will relay this information to the contractor and contracting officer for further action. Investigations for contractor employees requiring access to classified information must be initiated by the contractor Facility Security Officer (FSO).

(3) The contracting officer will ensure that the respective DLA Intelligence Personnel Security Office initiates investigations for contractor employees not requiring access to classified information (i.e., IT or unescorted entry).

(4) It is the contractor's responsibility to ensure that adequate information is provided and that each contractor employee completes the appropriate paperwork, as required either by the contracting officer or the DLA Intelligence Personnel Security Office, in order to begin the investigation process for the required clearance level.

(e) The contractor is responsible for ensuring that each contractor employee assigned to the position has the appropriate security clearance level.

(f) The contractor shall submit each request for IT access and investigation through the contracting officer to the assigned or cognizant DLA Intelligence Personnel Security Office. Requests shall include the following information and/or documentation:

(1) Standard Form (SF) 85, Questionnaire for Non-Sensitive Positions, or the SF 86, Questionnaire for National Security Positions (see note below);

(2) Proof of citizenship (i.e., an original or a certified copy of a birth certificate, passport, or naturalization certificate); and

(3) Form FD-258, Fingerprint Card (however, fingerprinting can be performed by the cognizant DLA Intelligence Personnel Security Office).

(Note to (f)(1) above: An investigation request is facilitated through use of the SF 85 or the SF 86. These forms with instructions as well as the Optional Form (OF) 306, Declaration for Federal Employment, which is required with submission of the SF85 or SF 86, are available at the Office of Personnel Management's (OPM) system called Electronic – Questionnaires for Investigations Processing (e-QIP). Hard copies of the SF85 and SF86 are available at OPM's web-site, www.opm.gov, but hard copies of the forms are not accepted.)

(g) Required documentation, listed above in paragraphs (f)(1) through (3), must be provided by the contractor as directed by the contracting officer to the cognizant DLA Intelligence Personnel Security Office at the time of fingerprinting or prior to the DLA Intelligence Personnel Security Office releasing the investigation to OPM.

(h) Upon completion of the NACI, NACLC, SSBI, or other sufficient, appropriate investigation, the results of the investigation will be forwarded by OPM to the appropriate adjudication facility for eligibility determination or the DLA Intelligence Personnel Security Office for review and determination regarding the applicant's suitability to occupy an unescorted entry position in performance of the DLA contract. Contractor personnel shall notcommence work on this effort until the investigation has been favorably adjudicated or the contractor employee has been waived into the position pending completion of adjudication. The DLA Intelligence Personnel Security Office will ensure that results of

investigations will be sent by OPM to the Department of Defense, Consolidated Adjudications Facility (DoDCAF) or DLA Intelligence Personnel SecurityOffice.

(i) A waiver for IT level positions to allow assignment of an individualcontractor employee tocommence work prior to completion of the investigation may be granted in emergencysituations when it is determined that a delay would be harmful to national security. A requestfor waiver will be considered only after the Governmentis in receipt of the individual contractor employee's completed forms, the background investigationhas been initiated, and favorable FBI fingerprint check has been conducted. The request for a waiver must be approved by the Commander/Director or Deputy Commander/Director of the site. The cognizant DLAIntelligence Personnel SecurityOffice reserves the right to determine whether a waiver request will be forwarded for processing. The individualcontractor employee for which the waiver is being requested maynot be assigned to a position, that is, physically workat the Federally-controlled facility and/or be granted access to Federally-controlledinformation systems, until the waiver has been approved.

(j)The requirements ofthisprocurement noteapply to the prime contractor and any subcontractors the prime contractor may employ during the course of this contract, as well asany temporary employees that may be hired by thecontractor. The Government retains the right to request removal ofcontractor personnel, regardless of prior clearance or adjudicationstatus whose actions, while assigned to this contract,who are determined by the contracting officer to conflictwith the interests ofthe Government. If such removal occurs, the contractor shall assign qualified personnel, with the required investigation, to any vacancy.

(k) Allcontractor personnel who are granted access to Government and/or Federally-controlled informationsystems shall observe all local automated information system (AIS)security policies and procedures. Violations of local AIS security policy, such as passwordsharing, performing personal work, file accessviolations, or browsing files outside the scopeof the contract, will result in removal of the contractor employee from Government propertyand referralto the contractorfor appropriatedisciplinary action. Actions taken by thecontractor in response to a violation will be evaluated and willbe reflected in the contractor'sperformance assessment for use in making future source selection decisions. In addition,based on the nature and extent of any violations of AIS security policy, the Government willconsider whether it needs to pursue any other actions under the contract such as a possibletermination.

(l) Thecontractor may also be required to obtain a Common Access Card (CAC) orInstallation Access Badge for eachcontractor employee in accordance with proceduresestablished by DLA. When a CAC is required, thecontracting officer will ensure thatthe contractor follows the requirements of Homeland Security Presidential Directive 12 and anyother CAC-related requirements in the contract. The contractor shall provide, on a monthly basis, a listing of all personnel working under the contractthat haveCACs.

(m) Contractor personnel must additionally receive operations security (OPSEC) andinformation security (INFOSEC) awareness training. The DLA annual OPSEC refresher training and DLA annual INFOSEC training will satisfy these requirements and are availablethrough the DLA Intelligence Office.

(n) When acontractor employee who has beengranted a clearance is removed from the contract, the contractor shall provide an appropriately trained substitute who has met or will meet the investigative requirements of this procurement note. The substitute may not begin work on the contract without written documentation, signed by the contracting officer, stating that the new contractor employee has met one of the criteria set forth in paragraphs (c), (d), or (i) of this procurement note (i.e., acceptance of a previously completed security investigation, satisfactory completion of a new investigation, or a waiver allowing work to begin pending completion of an

investigation). Contractor individual employees removed from this contract as a result of a violation of local AIS security policy are removed for the duration of the contract.

(o) The following shall be completed for every employee of the Government contractor working on this contract upon contract expiration. Additionally, the contractor shall notify the contracting officer immediately in writing whenever a contractor employee working on this contract resigns, is reassigned, is terminated, or no longer requires admittance to the Federally-controlled facility or access to Federally-controlled information systems. When the contractor employee departs, the contractor will relay departure information to the cognizant DLA Intelligence Personnel Security Office and the Trusted Agent (TA) that entered the individual into the Trusted Associated Sponsorship System (TASS), so appropriate databases can be updated. The contractor will ensure each departed employee has completed the DLA J6 Out-Processing Checklist, when applicable, for the necessary security briefing, has returned any Government-furnished equipment, returned the DoD CAC and DLA (or equivalent Installation) badge, returned any DoD or DLA vehicle decal, and requested deletion of local area network account with a prepared Department of Defense (DD) Form 2875. The contractor will be responsible for any costs involved for failure to complete the out-processing, including recovery of Government property and investigation involved.

(p) These contractor security requirements do not excuse the contractor from meeting the delivery schedule/performance requirements set forth in the contract, or waive the delivery schedule/performance requirements in any way. The contractor shall meet the required delivery schedule/performance requirements unless the contracting officer grants a waiver or extension.

(q) The contractor shall not bill for personnel, who are not working on the contract while that contractor employee's clearance investigation is pending.

*****

SUBPART 4.16 – UNIQUE PROCUREMENT INSTRUMENT IDENTIFIERS

(Revised September 9, 2016 through PROCLTR 2016-09)

4.1601 Policy.

(a) This process, for Business Process Analyst use only, is located in the Procurement Job Aid applicable to PIIN maintenance in EP and ECC:

Supplier Relationship Management (SRM)/EProcurement:

Table Maintenance - Maintaining PIIN Tables (https://dlamil.dps.mil/sites/InfoOps/Shared Documents/Forms/AllItems.aspx?FolderCTID=0x012000D3D259D71343A94E992AA17310CB0231&viewid=bb1b25a6%2D56d8%2D4398%2Dac48%2D5f987c946cca&id=%2Fsites%2FInfoOps%2FShared Documents%2FEBS ONLINE HELP%2FePROCUREMENT%2FTable Maintenance)

Table Maintenance - Maintaining Basic Agreement PIIN/SPIIN Tables (https://dlamil.dps.mil/sites/InfoOps/Shared Documents/Forms/AllItems.aspx?FolderCTID=0x012000D3D259D71343A94E992AA17310CB0231&viewid=bb1b25a6%2D56d8%2D4398%2Dac48%2D5f987c946cca&id=%2Fsites%2FInfoOps%2FShared Documents%2FEBS ONLINE HELP%2FePROCUREMENT%2FTable Maintenance).

Enterprise Core Component (ECC):

Table Maintenance - PIIN and Call Number Table Maintenance and Associated Error Workflow Tables (https://dlamil.dps.mil/sites/InfoOps/Shared Documents/Forms/AllItems.aspx?FolderCTID=0x012000D3D259D71343A94E992AA17310CB0231&viewid=bb1b25a6%2D56d8%2D4398%2Dac48%2D5f987c946cca&id=%2Fsites%2FInfoOps%2FShared Documents%2FEBS ONLINE HELP%2FPROCUREMENT DOCUMENTS%2FTable Maintenance).

SUBPART 4.71 – UNIFORM CONTRACT LINE ITEM NUMBERING SYSTEM

4.7103-2 Numbering procedures.

DEVIATION 20-01 authorizes DLA Disposition Services to use a hazardous waste (HW) Profile-Based CLIN/sub-CLIN numbering structure. This deviation expires on November 17, 2022.

4.7104-2 Numbering procedures.

Reference 4.7103-2.

SUBPART 4.73—SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

(Revised March 23, 2020 through PROCLTR 2020-01)

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.”

4.7302 Policy.

(S-90) Contracting officers, in coordination with the requiring activity, shall consider using an evaluation factor to assess an offeror's cybersecurity preparedness, and/or using a statement of work (SOW) requirement to address postaward cybersecurity verification and validation.

(1) Contracting officers shall document in the acquisition plan the rationale for deciding whether or not to use a cybersecurity evaluation factor and SOW requirement.

(2) Contracting officers shall use a cybersecurity evaluation factor when the acquisition provides operationally critical support, or when a risk assessment indicates potential impact to operations if a contractor experiences a cybersecurity breach or is unable to execute contract requirements due to a cyber incident. Contracting officers shall use the SOW requirement when a cybersecurity evaluation factor is used. Contracting officers may use the SOW requirement without a cybersecurity evaluation

factor when the Government may benefit from postaward verification and validation of a contractor's cybersecurity preparedness.

(3) Contracting officers shall use the Cybersecurity Evaluation Factor and Statement of Work (SOW) Requirement ; (https://dlamil.dps.mil/sites/Acquisition/SharedDocuments/Forms/AllItems.aspx?RootFolder=%2Fsites%2FAcquisition%2FSharedDocuments%2FJ%2D73%2FCybersecurityEvaluation&FolderCTID=0x01200080FADA3E9BBF764593CF2E25DC6FA477&View=%7BE9B41126%2DD28F%2D4F87%2DA9F7%2DDDF914A82406%7D), unless the contracting officer obtains approval from DLA Information Operations to use a tailored cybersecurity evaluation factor and SOW requirement.

(4) Contracting officers shall identify to the DLA Acquisition Operations Division all solicitations that will include a cybersecurity evaluation factor and/or the SOW requirement.

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 25.79.

(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 4.7303-3(a)(S-91)(i)(B)); and

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