DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

June 2, 2018

PROCLTR 2018- 11

MEMORANDUM FOR PROCLTR DISTRIBUTION LIST

SUBJECT: Safeguarding Covered Defense Information and Cyber Incident Reporting (Defense Logistics Acquisition Directive (DLAD) Subpart 4.73)

This PROCLTR issues new policy in section 4.7302 that requires contracting officers, in coordination with the requiring activity, to consider using an evaluation factor to assess an offeror's cybersecurity preparedness and/or a statement of work (SOW) requirement to address postaward cybersecurity verification and validation. The contracting officer must document the rationale for deciding whether or not to use a cybersecurity evaluation factor and SOW requirement in the acquisition plan; and identify all solicitations that will include a cybersecurity evaluation factor and/or SOW requirement to the DLA Acquisition Operations Division. The policy provides a link to the cybersecurity evaluation factor and SOW requirement on the SharePoint Acquisition – J7 page.

This PROCLTR revises section 4.7303-1 to identify requiring activity responsibilities in accordance with DFARS PGI 204.7303-1. The policy identifies other DLA requiring activity responsibilities, such as submitting the Special Situation Report (SITREP) in accordance with DLA DTM 17-017, Commander's Critical Information Requirements (CCIR) Reporting Policy Changes; submitting the Department of Defense Cyber Crime Center (DC3) cyber incident notification to the DLA Computer Emergency Response Team; coordinating with the Damage Assessment Management Office; taking appropriate actions to mitigate risks identified in the damage assessment report; and updating the Program Protection Plan. If the requiring activity is external to DLA, the contracting officer submits the Special SITREP and DC3 cyber incident notification. The policy provides a link to the instructions and template for submitting the Special SITREP on the SharePoint Acquisition – J6 page. The DLA Information Operations Cyber Security Team Manager/System Security Engineer helps the DLA requiring activity assess the risk and mitigation strategy; and consults with the contracting officer before assessing contractor compliance with DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

This PROCLTR is effective immediately. This PROCLTR revises the DLAD as stated in the attachment, which takes precedence over the published DLAD until this revision is incorporated in the published version. Please ensure widest distribution of this PROCLTR to your acquisition workforce, and include the information in your training materials. The point of contact is Milissa Dart, DLA Acquisition Compliance, Policy and Pricing Division, J72, (571) 767-2544, DSN (392) 767-2544, or email: milissa.dart@dla.mil.

BEEBE.MATTHEW.RICHARD.1012725473

Digitally signed by BEEBE.MATTHEW.RICHARD.1012725473
Date: 2018.06.02 11:44:17 -04'00'

MATTHEW R. BEEBE
Director, DLA Acquisition

Attachment:
As stated

DEFENSE LOGISTICS ACQUISITION DIRECTIVE
PART 4 – ADMINISTRATIVE MATTERS

CONFORMED VERSION

TABLE OF CONTENTS

SUBPART 4.73—SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

4.7301 Definitions.
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."

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 SOW requirement provided on the DLA Acquisition page at https://dlamil.dps.mil/sites/Acquisition/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2FAcquisition%2FShared%20Documents%2FJ%2D73%2FCybersecurity%20Evaluation&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.
(S-90) The requiring activity will notify the contracting officer when a solicitation is expected to result

in a contract, task order, or delivery order that will involve covered defense information or operationally critical support (see DFARS PGI 204.7303-1). 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.

(S-91) DLA requiring activities shall—

(1) Identify to the contracting officer whether or not the requirement includes covered defense information or operationally critical support.

(2) Ensure the contracting officer handles all direct communications with the contractor regarding the cyber incident.

(3) Submit a Special Situation Report (Special SITREP) in accordance with DLA DTM 17-017, Commander's Critical Information Requirements (CCIR) Reporting Policy Changes. Instructions and template for submitting this report are available at https://dlamil.dps.mil/sites/InfoOps/CCIR/Forms/AllItems.aspx. Provide the Department of Defense Cyber Crime Center (DC3) cyber incident notification to the DLA Computer Emergency Response Team (CERT) (cert@dla.mil).

(4) Contact the Damage Assessment Management Office (DAMO) (phone: OSD Liaison 410-694-4380) to receive point of contact information, if the DAMO has not already initiated contact.

(5) Coordinate with the DAMO regarding requests for contractor media, which must be submitted within 90 days following any reported compromises of DoD unclassified CDI. Notify the contracting officer of the decision whether or not to request media, and provide the rationale.

(6) Assess and implement appropriate programmatic, technical, and operational actions to mitigate risks identified in the damage assessment report. Update the Program Protection Plan to reflect any changes as a result of the assessment.

(S-92) If the requiring activity is external to DLA, the contracting officer shall submit a Special SITREP and provide the DC3 cyber incident notification (see 4.7303-1(S-91)(3)).

(S-93) The DLA J61 Information Operations Cyber Security Team Manager/System Security Engineer shall—

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

(2) Consult with the contracting officer before assessing contractor compliance with the requirements of DFARS 252.204-7012.

* * * * *

MARKED VERSION

TABLE OF CONTENTS

* * * * *

* * * * *

SUBPART 4.73—SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

[4.7301 Definitions.
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."

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 SOW requirement provided on the DLA Acquisition page at https://dlamil.dps.mil/sites/Acquisition/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2FAcquisition%2FShared%20Documents%2FJ%2D73%2FCybersecurity%20Evaluation&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.

~~The requiring activity for DLA-managed items varies, but generally will be the organization or activity submitting the requirement.~~

[(S-90) The requiring activity will notify the contracting officer when a solicitation is expected to result in a contract, task order, or delivery order that will involve covered defense information or operationally critical support (see DFARS PGI 204.7303-1). 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.

(S-91) DLA requiring activities shall—

(1) Identify to the contracting officer whether or not the requirement includes covered defense information or operationally critical support.

(2) Ensure the contracting officer handles all direct communications with the contractor regarding the cyber incident.

(3) Submit a Special Situation Report (Special SITREP) in accordance with DLA DTM 17-017, Commander's Critical Information Requirements (CCIR) Reporting Policy Changes. Instructions and template for submitting this report are available at:

https://dlamil.dps.mil/sites/InfoOps/CCIR/Forms/AllItems.aspx. Provide the Department of Defense Cyber Crime Center (DC3) cyber incident notification to the DLA Computer Emergency Response Team (CERT) (cert@dla.mil).

(4) Contact the Damage Assessment Management Office (DAMO) (phone: OSD Liaison 410-694-4380) to receive point of contact information, if the DAMO has not already initiated contact.

(5) Coordinate with the DAMO regarding requests for contractor media, which must be submitted within 90 days following any reported compromises of DoD unclassified CDI. Notify the contracting officer of the decision whether or not to request media, and provide the rationale.

(6) Assess and implement appropriate programmatic, technical, and operational actions to mitigate risks identified in the damage assessment report. Update the Program Protection Plan to reflect any changes as a result of the assessment.

(S-92) If the requiring activity is external to DLA, the contracting officer shall submit a Special SITREP and provide the DC3 cyber incident notification (see 4.7303-1(S-91)(3)).

(S-93) The DLA J61 Information Operations Cyber Security Team Manager/System Security Engineer shall—

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

(2) Consult with the contracting officer before assessing contractor compliance with the requirements of DFARS 252.204-7012.]

~~**4.7303-2 Safeguarding controls and requirements.**~~

~~Provide a copy of the submission to J6 Cybersecurity for DLA managed items. DLR contracting officers provide a copy of the submission to the Military Service CIO.~~

~~**4.7303-3 Cyber incident and compromise reporting.**~~

~~(a)(1) The contracting officer shall also send the incident report for DLA managed items via encrypted e-mail to DLACyberIncidentReport@dla.smil.mil and copy their supervisor, and DLR contracting officers shall also send a copy of the incident report to the Military Service CIO. The contract file shall be documented accordingly.~~

~~(a)(3)(i) Consultation and assessment will be performed for DLA managed items by the J6 Cybersecurity and DLA Intelligence Office. Include the requiring activity for DLA managed items.~~

~~(c) Email requests for DLA managed items encrypted to the contractors and DLACyberIncidentReport@dla.smil.mil.~~

~~**4.7303-4 DoD damage assessment activities.**~~

~~Email correspondence for DLA managed items encrypted to DLACyberIncidentReport@dla.smil.mil.~~

* * * * *