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).

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