<?xml encoding="UTF-8">

PGI 204.7303-3 Cyber incident and compromise reporting.

(a) When a cyber incident is reported by a contractor, the DoD Cyber Crime Center (DC3) will send an unclassified encrypted email containing the cyber incident report to the contracting officer(s) identified on the Incident Collection Format (ICF). The DC3 may request the contracting officer send a digitally signed e-mail to DC3.

(1) The procuring contracting officer (PCO) shall notify the requiring activities that have contracts identified in the ICF. In cases where an administrative contracting officer (ACO) receives the cyber incident report, in lieu of the PCO, the ACO shall notify the PCO for each affected contract, who will then notify the requiring activity.

(2) In cases of cyber incidents involving multiple contracts, the DoD components will collaboratively designate a single contracting officer to coordinate additional actions required of the contractor, on behalf of the affected DoD components. The requiring activity will notify the contracting officer once a lead is designated.

(3) If the requiring activity requests an assessment of compliance with the requirements of the clause at DFARS 252.204-7012 related to the cyber incident, the contracting officer shall—

(i) Consult with the DoD component Chief Information Officer (CIO)/cyber security office;

(ii) Request a description of the contractor's implementation of the security requirements in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) in order to support evaluation of whether any of the controls were inadequate, or if any of the controls were not implemented at the time of the incident; and

(iii) Provide a copy of the assessment of contractor compliance to the requiring activity, the DoD CIO at osd.dibcsia@mail.mil, and the other contracting officers listed in the cyber incident report.

(b) When requested by the contractor, the contracting officer shall provide the contractor with the "Instructions for Malware Submission" document available at http://www.acq.osd.mil/dpap/pdi/docs/Instructions_for_Malware_Submissio…. The contracting officer should never receive malicious software directly from the contractor.

(c) If the requiring activity requests access to contractor information or equipment, in accordance with DFARS 252.204-7012(f), the contracting officer shall provide a written request to the contractor.

(d) For additional information on cyber incident reporting, see the Frequently Asked Questions document at http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contr….

Parent topic: PGI 204.7303 Procedures.