PGI 239.7603-3 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 to send a digitally signed email 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 work together to designate a single contracting officer to coordinate the effort. The requiring activity will notify the contracting officer once a lead is designated.

(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/dars/pgi/docs/Instructions_for_Submitting_M.... 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 252.239-7010(g), the contracting officer shall provide a written request to the contractor.

(d) For additional information on cyber incident reporting, see the frequently asked question document at http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contr....

Parent topic: PGI 239.7603 Procedures.