PGI 204.73 -SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

Parent topic: PGI Part 204 - ADMINISTRATIVE AND INFORMATION MATTERS

PGI 204.7303 Procedures.

PGI 204.7303-1 General.

(a) The contracting officer will be notified by the requiring activity when a solicitation is expected to result in a contract, task order, or delivery order that will involve—

(1) Covered defense information; or

(2) Operationally critical support.

(b) The contracting officer shall—

(1) Ensure that the requiring activity provides a work statement or specification that includes the identification of covered defense information or operationally critical support consistent with paragraph (a).

(2) Ensure that the solicitation and resultant contract, task order, or delivery order includes the requirement (such as a contract data requirements list), as provided by the requiring activity, for the contractor to apply markings, when appropriate, on covered defense information.

PGI 204.7303-2 Safeguarding controls and requirements.

(a) When an offeror proposes to vary from any of the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” in accordance with paragraph (c)(2) of the solicitation provision at DFARS 252.204-7008, or in accordance with paragraphs (b)(2)(ii)(B) of DFARS clause 252.204-7012, the contracting officer shall submit the offeror’s explanation of the proposed variance to the DoD Chief Information Officer via email at osd.dibcsia@mail.mil for adjudication.

(b) For additional information on safeguarding controls and requirements, see the Frequently Asked Questions document at http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contr....

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....

PGI 204.7303-4 DoD damage assessment activities.

(a) Prior to initiating damage assessment activities, the contracting officer shall verify that any contract identified in the cyber incident report includes the clause at DFARS 252.204-7012. If the contracting officer determines that a contract identified in the report does not contain the clause, the contracting officer shall notify the requiring activity that damage assessment activities, if required, may be determined to constitute a change to the contract.

(b) In cases of cyber incidents involving multiple contracts, a single contracting officer will be designated to coordinate with the contractor regarding media submission (see 204.7303-3 (a)(2)).

(c) If the requiring activity requests the contracting officer to obtain media, as defined in DFARS 252.204-7012, from the contractor, the contracting officer shall—

(1) Provide a written request for the media;

(2) Provide the contractor with the “Instructions for Media Submission” document available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_M...; and

(3) Provide a copy of the request to DC3, electronically via email at dcise@dc3.mil, and the requiring activity.

(d) If the contracting officer is notified by the requiring activity that media are not required, the contracting officer shall notify the contractor and simultaneously provide a copy of the notice to DC3 and the requiring activity.

(e) The contracting officer shall document the action taken as required by paragraph (c) or (d) of this section, in the contract file.

(f) Upon receipt of the contractor media, DC3 will confirm receipt in writing to the contractor and the requesting contracting officer.

(g) Once the requiring activity determines that the damage assessment activities are complete, the requiring activity will provide the contracting officer with a report documenting the actions taken to close out the cyber incident.