(Revised November 18, 2015)

PGI 204.73—SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

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 that will require covered defense information to be furnished by the Government and/or developed or delivered by the contractor, or when the contractor will provide operationally critical support.

(b) The contracting officer shall—

(1) Ensure that covered defense information or operationally critical support, for which notification was provided in accordance with paragraph (a), is identified in the contract, task order, or delivery order;

(2) Ensure that the 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; and

(3) Coordinate with the requiring activity for instruction regarding the disposition of covered defense information associated with the contract. In cases where contract administration has been delegated to an administrative contracting officer (ACO), the ACO shall request the cognizant procuring contracting officer (PCO) to coordinate with the requiring activity.

(c) The safeguarding requirements and procedures apply until such time as the covered defense information designation is changed or removed by the requiring activity.

PGI 204.7303-2 Safeguarding controls and requirements.

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

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 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.

(3) If requested by the requiring activity to assess compliance with the requirements of the clause at DFARS 252.204-7012, 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 National Institute of Standards and Technology (NIST) Special Publication (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, 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_Submission.docx. 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_contracting.html.

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.

(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_Media.docx; 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) When the requiring activity determines that the damage assessment activities are complete, the requiring activity will provide the contracting officer with a report documenting the findings from the damage assessment activities affecting covered defense information.

(h) The contracting officer shall include the report documenting the findings in the contract file(s) and provide a copy to the contractor.

(Added November 18, 2015)

PGI 239.76—CLOUD COMPUTING

PGI 239.7602 Policy and responsibilities.

PGI 239.7602-1 General.

(c)(6) When the clause at DFARS 252.239-7010 applies, the contracting officer shall provide the contractor with the name of the responsible Government official to contact in response to any spillage occurring in connection with the cloud computing services being provided. The requiring activity will provide the contracting officer with the name of the responsible official in accordance with agency procedures, as required by Enclosure 7 of DoDM 5200.01-V3, DoD Information Security Program: Protection of Classified Information.

PGI 239.7602-2 Required storage of data within the United States or outlying areas.

(b) Prior to authorizing storage of data outside the United States and outlying areas, the contracting officer must receive written authorization from the authorizing official.

PGI 239.7603 Procedures.

PGI 239.7603-1 General.

(a) When the apparently successful offeror indicates in the provision at DFARS 252.239-7009 that cloud computing services will be used in the performance of the contract, the contracting officer shall review the DoD Cloud Service Catalog at http://www.disa.mil/Computing/Cloud-Services/Cloud-Support (look under the "Additional Information" tab for "Service Catalog") to verify that the cloud service provider's offering to be used in the performance of the contract has a provisional authorization prior to award (see DFARS 239.7602-1(b)).

(b) When the contractor indicated in the provision at DFARS 252.239-7009 that it did not anticipate the use of cloud computing services in the performance of the contract and requests, after award, in accordance with the clause at DFARS 252.239-7010(b)(1), that the contracting officer approve the use of cloud computing services in the performance of the contract, the contracting officer shall—

(1) Request approval from the requiring activity for the contractor to use cloud computing services; and

(2) If the requiring activity provides approval, review the DoD Cloud Service Catalog at http://www.disa.mil/Computing/Cloud-Services/Cloud-Support (look under the "Additional Information" tab for "Service Catalog") to verify that the cloud service provider's offering to be used in the performance of the contract has a provisional authorization (see DFARS 239.7602-1(b)).

PGI 239.7603-2 Notification of third party access requests.

When a contractor provides notification of a request from a third party for access to

Government data or Government-related data, in accordance with DFARS 252.239-7010(j), the contracting officer shall convey the request to the requiring activity. The requiring activity will coordinate a response with the mission or data owner.

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_Malware.docx. 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_contracting.html.

PGI 239.7603-4 DoD damage assessment activities.

(a) Prior to initiating damage assessment activities, the contracting officer shall verify that a contract(s) identified in the cyber incident report include(s) the clause at DFARS 252.239-7010. 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.

(c) If the requiring activity requests the contracting officer obtain media, as defined at DFARS 252.239-7010, 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_Media.docx; 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) When the requiring activity determines that the damage assessment activities are complete, the requiring activity will provide the contracting officer with a report documenting the findings from the damage assessment activities affecting covered defense information.

(h) The contracting officer shall include the report documenting the findings in the contract file(s) and provide a copy to the contractor.