(Added December 12, 2014)

PGI 204.73—SAFEGUARDING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION

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 unclassified controlled technical information (CTI) to be furnished by the Government and/or developed by the contractor.

(b) The contracting officer shall—

(1) Notify the requiring activity that all DoD unclassified CTI provided to the contractor shall be marked with the appropriate distribution statement B-F (see DoDI 5230.2, Distribution Statements on Technical Documents);

(2) Ensure that the contract, task order, or delivery order includes a requirement (such as a contract data requirements list) for the contractor to apply the appropriate distribution statement(s) on any unclassified CTI developed by the contractor; and

(3) Coordinate with the requiring activity for instruction regarding the disposition of unclassified CTI 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 to the unclassified CTI until such time as the distribution statement identifying information as unclassified CTI (distribution statement B-F) is changed or removed by the controlling DoD office.

PGI 204.7303-2 Safeguarding controls.

(a) The DoD Chief Information Officer (CIO) is responsible to ensure contractor information systems are assessed in a standard way. When a contractor provides a written explanation that either DFARS 252.204-7012(b)(1)(ii)(A) or (B) apply, the contracting officer shall send the written explanation to the requiring activity and the DoD CIO at osd.dibcsia@mail.mil for adjudication and response.

(b) Table 1 of DFARS clause 252.204-7012 requires that contracting officers not specify the values that contractors may assign to the controls; they are applied to the contractor's internal information technology system, and cannot be subject to change from contract to contract.

(c) For additional information on the safeguarding controls, see the Frequently Asked Questions document at: http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf

PGI 204.7303-3 Cyber incident and compromise reporting.

(a) When a cyber incident is reported by a contractor, the Defense Cyber Crime Center (DC3) will send an unclassified encrypted email containing the DIBNet-generated Incident Collection Form (ICF) to the contracting officer(s) identified on the ICF. The Defense Cyber Crime Center may request the contracting officer to send a digitally signed e-mail to DC3 in order to enable the contracting officer to read the ICF.

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

(2) The requiring activity may request that the contracting officer assess contractor compliance with the requirements of DFARS 252.204-7012, in accordance with DFARS 204.7302(b)(2). In cases of cyber incidents involving multiple contracts, a single contracting officer will be designated and notified by a requiring activity. If requested to assess compliance, the contracting officer shall—

(i) Consult with the security manager, as identified by the requiring activity. The security manager is knowledgeable in cybersecurity and NIST-SP 800-53. This particular aspect of the security manager's role is also referred to as an information systems security engineer (ISSE) and may reside in Program Management Offices (PMOs), Program Executive Offices (PEOs), Air Force Network Integration Center (AFNIC), Space and Naval Warfare Systems Command (SPAWAR), US Army Network Enterprise Technology Command (NETCOM), DISA Field Security Operations (FSO), or elements performing similar functions within a Component. In Program Management Offices, security managers typically ensure that the program's information assurance/cybersecurity requirements are incorporated into the design of the system/product and are realized throughout development and production. Elsewhere, security managers are typically those who validate/certify that information systems meet information assurance/cybersecurity requirements prior to (and periodically during) operation); and

(ii) Consider the following options, if additional information is necessary to assess contractor compliance:

(A) Request a description of the implementation of the controls in DFARS 252.204-7012, *Table 1 – Minimum Security Controls for Safeguarding*, including requesting specific values (if not already requested prior to award), 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.

(B) Request the contractor's assessment of the cause of the cyber incident, e.g., what, if any, security control was inadequate or circumvented. As indicated in DFARS 204.7302(b)(2), a cyber incident does not imply that the contractor

has failed to provide adequate information safeguards for unclassified CTI, or has otherwise failed to meet the requirements of the clause at DFARS 252.204-7012.

(iii) Provide a copy of the assessment of contractor compliance to the requiring activity and to the DoD CIO, osd.dibcsia@mail.mil. A copy of the assessment will be provided to other contracting officers listed on the ICF by their respective requiring activity.

PGI 204.7303-4 DoD damage assessment activities.

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

(1) 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—

(i) Provide a written request for the media;

(ii) Provide the contractor with the "Instructions for Media Submission" document available here; and

(iii) Provide a copy of the request to DC3 (dcise@dc3.mil) and the requiring activity.

(2) 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.

(3) The contracting officer shall document the action taken as required by paragraph (a)(1) or (2) of this section, in the contract file.

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

(c) The requiring activity will provide the contracting officer with a report documenting the findings from the damage assessment activities affecting unclassified CTI.

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

PGI 204.7303-5 Subcontracts.

(a) The incident reporting required at DFARS 252.204-7012(d)(1) will be submitted by the prime contractor to the DoD via http://dibnet.dod.mil within 72 hours of notification from the subcontractor of any cyber incident.

(b) If a contractor is hosting unclassified CTI in the capacity as both a prime contractor and a subcontractor, and if the contractor is unable to determine specifically which contract effort is being impacted by the cyber incident, the contractor is required

to report to both the prime as a subcontractor, and to the DoD via http://dibnet.dod.mil as a prime contractor.