SUBPART 204.73—SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

(Revised September 21, 2015)

204.7300 Scope.

(a) This subpart applies to contracts and subcontracts requiring contractors and subcontractors to safeguard covered defense information that resides in or transits through covered contractor information systems by applying specified network security controls. It also requires reporting of cyber incidents.

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.

204.7301 Definitions.

As used in this subpart—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified information that—

(1) Is—

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(2) Falls in any of the following categories:

(i) *Controlled technical information.*

(ii) *Critical information (operations security).* Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(iii) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations, and munitions list; license applications; and sensitive nuclear technology information.

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Operationally critical support" means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

"Rapid(ly) report(ing)" means within 72 hours of discovery of any cyber incident.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

204.7302 Policy.

(a) DoD and its contractors and subcontractors will provide adequate security to safeguard covered defense information on their unclassified information systems from unauthorized access and disclosure.

(1) Contractors and subcontractors are required to submit to DoD—

(i) A cyber incident report;

(ii) Malicious software, if detected and isolated; and

(iii) Media (or access to covered contractor information systems and equipment) upon request.

(2) Contracting officers shall refer to PGI 204.7303-4(a)(1)(ii) for instructions on contractor submissions of media and malicious software.

(b) Subcontractors are required to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and to the prime contractor. Subcontractors shall provide the incident report number from DoD to the prime contractor. Lower-tier subcontractors are required to likewise report the same information to their higher-tier subcontractor, until the prime contractor is reached.

(c) The Government acknowledges that information shared by the contractor under these procedures may include contractor attributional/proprietary information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the contractor that reported the information. The Government shall protect against the unauthorized use or release of information that includes contractor attributional/proprietary information.

(d) A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate information safeguards for covered defense information on their unclassified information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012. When a cyber incident is reported, the contracting officer shall consult with the DoD component CIO/cyber security office prior to assessing contractor compliance (see PGI 204.7303-3(a)(2)). The contracting officer shall consider such cyber incidents in the context of an overall assessment of a contractor's compliance with the requirements of the clause at 252.204-7012.

(e) Support services contractors directly supporting Government activities related to safeguarding covered defense information and cyber incident reporting (e.g., providing forensic analysis services, damages assessment services, or other services that require access to data from another contractor) are subject to restrictions on use and disclosure.

204.7303 Procedures.
Follow the procedures relating to safeguarding covered defense information at PGI 204.7303.

204.7304 Solicitation provision and contract clauses.

Use the provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls (DEVIATION 2016-O0001)(OCT 2015) and the clause at 252.204-7012, Limitations on the Use or Disclosure of Third-Party Contractor Information (DEVIATION 2016-O0001)(OCT 2015), in lieu of the provision at DFARS 252.204-7008 and the clause at DFARS 252.204-7012. This class deviation remains in effect until incorporated in the DFARS or otherwise rescinded.

(a) Use the provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items.

(b) Use the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Information, in all solicitations and contracts for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting.

(c) Use the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items.