Subpart 204.73 - SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

Parent topic: Part 204 - ADMINISTRATIVE AND INFORMATION MATTERS

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 requirements. 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 unclassified 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 controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

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

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

“Media” means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

“Rapidly report” 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 252.227-7013 , Rights in Technical Data-Other Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in the 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)(1) Contractors and subcontractors are required to provide adequate security on all covered contractor information systems.

(2) Contractors required to implement NIST SP 800-171, in accordance with the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber incident Reporting, are required at time of award to have at least a Basic NIST SP 800-171 DoD Assessment that is current (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7019).

(3) The NIST SP 800-171 DoD Assessment Methodology is located at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171 .

(4) High NIST SP 800-171 DoD Assessments will be conducted by Government personnel using NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information.”

(5) The NIST SP 800-171 DoD Assessment will not duplicate efforts from any other DoD assessment or the Cybersecurity Maturity Model Certification (CMMC) (see subpart 204.75), except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

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

reached.

(1) If a cyber incident occurs, contractors and subcontractors 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 (c) for instructions on contractor submissions of media and malicious software.

(c) Information shared by the contractor 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 security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012 , Safeguarding Covered Defense Information and Cyber Incident Reporting. When a cyber incident is reported, the contracting officer shall consult with the DoD component Chief Information Officer/cyber security office prior to assessing contractor compliance (see PGI 204.7303-3 (a)(3)). 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., forensic analysis, damage assessment, or other services that require access to data from another contractor) are subject to restrictions on use and disclosure of reported information.

204.7303 Procedures.

(a) Follow the procedures relating to safeguarding covered defense information at 204.7303

(b) The contracting officer shall verify that the summary level score of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old, unless a lesser time is specified in the solicitation) (see 252.204-7019) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted in Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/), prior to—

(1) Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800-171 in accordance with the clause at 252.204-7012; or

(2) Exercising an option period or extending the period of performance on a contract, task order, or delivery order with a contractor that is that is required to implement the NIST SP 800-171 in accordance with the clause at 252.204-7012.

204.7304 Solicitation provision and contract clauses.

(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 products and commercial services, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(b) Use the clause at 252.204-7009 , Limitations on the Use or Disclosure of Third- Party Contractor Reported Cyber Incident Information, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, 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 products and commercial services, except for solicitations and contracts solely for the acquisition of COTS items.

(d) Use the provision at 252.204-7019 , Notice of NIST SP 800-171 DoD Assessment Requirements, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(e) Use the clause at 252.204-7020 , NIST SP 800-171 DoD Assessment Requirements, in all solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those that are solely for the acquisition of COTS items.