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.

Parent topic: Subpart 204.73 - SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING