1239.7002 Policy.

(a) Contractors and subcontractors are required to provide adequate security on all contractor information systems that will collect, use, process, store, or disseminate DOT sensitive data.

(b) Contractors and subcontractors shall report cyber incidents directly to DOT via the DOT Security Operations Center (SOC) 24 hours-a-day, 7 days-a-week, 365 days a year (24x7x365) at phone number: 571–209–3080 (Toll Free: 866–580–1852) within two (2) hours of discovery. Subcontractors will provide to the prime contractor the incident report number automatically assigned by DOT. Lower-tier subcontractors likewise report the incident report number automatically assigned by DOT to their higher-tier subcontractor, until the prime contractor is reached.

(c) If a cyber incident occurs, contractors and subcontractors shall submit to DOT, in accordance with the instructions contained in the clause at 1252.239–74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting—

(1) A cyber incident report;

(2) The malicious software, if detected and isolated; and

(3) The medium or media (or access to covered contractor information systems and equipment) upon request.

(d) Notwithstanding the requirement in this subpart for the reporting of cyber incidents, if existing safeguards have ceased to function or the Government or Contractor discovers new or unanticipated threats or hazards, the discoverer shall immediately bring the situation to the attention of the other party.

(1) Information shared by the contractor may include contractor attributional/proprietary information. The Government will protect against the unauthorized use or release of information that includes contractor attributional/proprietary information.

(2) 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 1252.239–74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting. When a cyber incident is reported, the contracting officer shall consult with the DOT component Chief Information Officer/cyber security office prior to assessing contractor compliance (*see* 1239.7003). 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 1252.239–74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting.

(3) Support services contractors directly supporting Government activities related to safeguarding DOT sensitive data 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 1239.70—Information Security and Incident Response Reporting