Subpart 1239.70—Information Security and Incident Response Reporting

Parent topic: PART 1239—ACQUISITION OF INFORMATION TECHNOLOGY

1239.7000 Scope of subpart.

(a) This subpart applies to contracts and subcontracts requiring contractors and subcontractors to safeguard DOT sensitive data 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.

1239.7001 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.

Contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits DOT sensitive information.

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

DOT sensitive data means unclassified information 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 DOT 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.

Rapidly report means reporting within two (2) hours of discovery of any cyber incident.

Technical information means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information. 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.

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.

1239.7003 Contract clauses.

(a) The contracting officer shall insert the clause at 1252.239–72, Compliance with Safeguarding DOT Sensitive Data 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) The contracting officer shall insert clause at 1252.239–73, 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 commercial services that include support for the Government's activities related to safeguarding DOT sensitive data and cyber incident reporting.

(c) The contracting officer shall insert clause at 1252.239–74, Safeguarding DOT Sensitive Data 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.