1252.239-74 Safeguarding DOT Sensitive Data and Cyber Incident Reporting.

As prescribed in 1239.7003(c), insert the following clause:

Safeguarding DOT Sensitive Data and Cyber Incident Reporting (NOV 2022)

(a) *Definitions.* As used in this clause—

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

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, whereby without authorization information is disclosed, modified, destroyed, lost, or copied to unauthorized media—whether intentionally or unintentionally.

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, trade secrets, commercial or financial information, or other commercially sensitive information not customarily shared outside of a company.

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

DOT sensitive data means unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulation, and Government-wide 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.

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.

Federal record as defined in 44 U.S.C. 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. The term Federal record—

(1) Includes all DOT records;

(2) Does not include personal materials;

(3) Applies to records created, received, or maintained by Contractors pursuant to a DOT contract; and

(4) May include deliverables and documentation associated with deliverables.

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

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

Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

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 DOT sensitive data is recorded, stored, or printed within a covered contractor information system.

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.

Spillage security incident means an incident that results in the transfer of classified or unclassified information onto an information system not accredited (*i.e.,* authorized) for the appropriate security level.

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, 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.

(b) *Adequate security.* The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered Contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 1252.239–76, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (*i.e.,* other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered Contractor information systems that are not part of an IT service or system operated

on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(iv) of this clause, the contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at *https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final*) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii) The Contractor shall implement NIST SP 800–171, Rev. 2, no later than 30 days after the award of this contract. The Contractor shall notify Contract Officer of any security requirements specified by NIST SP 800–171, Rev. 2 not implemented within 30 days of time of contract award.

(iii) If the Offeror proposes to vary from any security requirements specified by NIST SP 800–171, Rev. 2 in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DOT Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How the Contractor will use an alternative, but equally effective, security measure to satisfy the requirements of NIST SP 800–171, Rev. 2.

(iv) The Office of the DOT CIO will evaluate offeror requests to vary from NIST SP 800–171, Rev. 2 requirements and inform the Offeror in writing of its decision before contract award. The Government will incorporate accepted variance(s) from NIST SP 800–171, Rev. 2 into any resulting contract.

(v) The Contractor need not implement any security requirement adjudicated by an authorized representative of the DOT CIO to be nonapplicable, or have an alternative, but equally effective, security measure that may be implemented in its place.

(vi) If the DOT CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when the Contractor requests its recognition under this contract

(3) If the Contractor intends to use an external cloud service provider to store, process, or transmit any DOT sensitive data in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (*https://www.fedramp.gov/resources/documents/*) and that the cloud service provider complies with requirements in paragraphs (c) through (h) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(4) The Contractor will apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (b)(2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (*e.g.,* medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan, as required by, clause 1252.239–70, Security

Requirements for Unclassified Information Technology Resources.

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the DOT sensitive data residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of DOT sensitive data, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised DOT sensitive data or whether the incident affects the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DOT Security Operations Center (SOC) 24x7x365 at phone number: 571–209–3080 (Toll Free: 1–866–580–1852).

(d) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DOT and shall include, at a minimum, the required elements in paragraph (c)(1)(i).

(e) *Spillage.* Upon notification by the Government of a spillage, or upon the Contractor's discovery of a spillage, the Contractor shall cooperate with the Contracting Officer to address the spillage in compliance with DOT policy.

(f) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, the Contractor shall submit the malicious software to DOT in accordance with instructions provided by the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(g) *Media preservation and protection.* When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DOT to request the media or decline interest.

(h) *Access to additional information or equipment necessary for forensic analysis.* Upon request by DOT, the Contractor shall provide DOT with access to additional information or equipment that is necessary to conduct a forensic analysis.

(i) *Cyber incident damage assessment activities.* If DOT elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (c) of this clause.

(j) *DOT safeguarding and use of Contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that includes Contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the Contractor attributional/proprietary information that is included in such authorized release consistent with

applicable law.

(k) *Use and release of Contractor attributional/proprietary information not created by or for DOT.* Information that is obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that is not created by or for DOT is authorized to be released outside of DOT—

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 1252.239–73, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information; or

(5) With Contractor's consent; or

(6) As otherwise required by law.

(l) *Use and release of Contractor attributional/proprietary information created by or for DOT.* Information that is obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that is created by or for DOT (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DOT for purposes and activities authorized by paragraph (j) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(m) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(n) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable Government statutory or regulatory requirements.

(o) *Subcontract flowdown requirements.* The Contractor shall—

(1) Include this clause, including this paragraph (o), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve DOT sensitive data, including subcontracts for commercial products and commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as DOT sensitive data and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800–171, Rev. 2 security requirement to the Contracting Officer, in accordance with

paragraph (b)(2)(iii) of this clause; and

(ii) Provide the incident report number, automatically assigned by DOT, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DOT as required in paragraph (c) of this clause.

(End of clause)

Parent topic: Subpart 1252.2—Text of Provisions and Clauses