PART 1239—ACQUISITION OF INFORMATION TECHNOLOGY

Authority: 5 U.S.C. 301; 41 U.S.C. 1121(c)(3); 41 U.S.C. 1702; and 48 CFR 1.301 through 1.304.

Source: 87 FR 61159, Oct. 7, 2022, unless otherwise noted.

1239.000 Scope of part.

1239.002 Definitions.

Subpart 1239.1—General

1239.101 Policy.

1239.101-70 Policy—software management and development.

1239.101-71 Scope.

1239.101-72 Definitions.

1239.101-73 Policy.

1239.106-70 Contract clauses.

Subpart 1239.2—Information and Communication Technology

1239.201 Scope of subpart.

1239.203 Applicability.

1239.203-70 Information and communication technology accessibility standards—contract clause and provision.

Subpart 1239.70—Information Security and Incident Response Reporting

1239.7000 Scope of subpart.

1239.7001 Definitions.

1239.7002 Policy.

1239.7003 Contract clauses.

Subpart 1239.71—Protection of Data About Individuals

1239.7100 Scope of subpart.

1239.7101 Definitions.

1239.7102 Policy.

1239.7103 Responsibilities.

1239.7104 Contract clause.

Subpart 1239.72—Cloud Computing

1239.7200 Scope of subpart.

1239.7201 Definitions.

1239.7202 Policy.

1239.7203 DOT FedRAMP specific requirements.

1239.7204 Contract clauses.

Subpart 1239.73—Technology Modernization and Upgrades/Refreshment

1239.7300 Scope of subpart.

1239.7301 Definitions.

1239.7302 Policy.

1239.7303 Contract clauses.

Subpart 1239.74—Records Management

1239.7400 Scope of subpart.

1239.7401 Definition.

1239.7402 Policy.

1239.7403 Contract clause.

Parent topic: SUBCHAPTER F—SPECIAL CATEGORIES OF CONTRACTING

1239.000 Scope of part.

In addition to FAR 39.000, this part prescribes acquisition policies and procedures for use in acquiring information technology and information technology-related supplies, services and systems, including information security, to include—

(a) Software management and development;

(b) Section 508 standards and compliance for contracts;

(c) Information security and incident response reporting;

(d) Protection of data about individuals;

(e) Cloud computing;

(f) Technology modernization and upgrade/refreshment; and

(g) Record management.

1239.002 Definitions.

As used in this part—

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

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 information is recorded, stored, or printed within an information system.

Subpart 1239.1—General

1239.101 Policy.

1239.101-70 Policy—software management and development.

1239.101-71 Scope.

This subpart applies to all acquisitions of products or services supporting the development or maintenance of software.

1239.101-72 Definitions.

As used in this subpart—

Application means software that resides above system software and includes applications such as database programs, word processors and spreadsheets. Application software may be bundled with system software or published alone.

Programming software means tools to aid developers in writing programs including compilers, linkers, debuggers, interpreters and text editors.

Software means a set of instructions or programs instructing a computer to do specific tasks including scripts, applications, programs and a set of instructions. Includes System, Programming, and Application software.

System software means a platform comprised of Operating System (OS) programs and services, including settings and preferences, file libraries and functions used for system applications. System software also includes device drivers that run basic computer hardware and peripherals.

1239.101-73 Policy.

The contracting officer will ensure all documents involving the acquisition of products or services supporting the development or maintenance of DOT software applications, systems, infrastructure, and services contain the appropriate clauses as may be required by Federal Acquisition Regulation (FAR) and other Federal authorities, in order to ensure that information system modernization is prioritized accordance with Federal law, OMB Guidance, and DOT policy.

1239.106-70 Contract clauses.

The contracting officer shall insert the clause at 1252.239–70, Security Requirements for Unclassified Information Technology Resources, and the clause at 1252.239–71, Information Technology Security Plan and Accreditation, in all solicitations and contracts exceeding the micro-purchase threshold that include information technology services.

Subpart 1239.2—Information and Communication Technology

1239.201 Scope of subpart.

This subpart applies to the acquisition of Information and Communication Technology (ICT) supplies and services. It concerns the access to and use of information and data, by both Federal employees with disabilities, and members of the public with disabilities in accordance with FAR 39.201. This subpart implements DOT policy on section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as it applies to contracts and acquisitions.

1239.203 Applicability.

(a) Solicitations for information and communication technology supplies and services may require submission of a section 508 Checklist available at *https://www.section508.gov/sell/vpat*.

1239.203-70 Information and communication technology accessibility standards—contract clause and provision.

(a) The contracting officer shall insert the provision at 1252.239–92, Information and Communication Technology Accessibility Notice, in all solicitations.

(b) The contracting officer shall insert the clause at 1252.239–93, Information and Communication Technology Accessibility, in all contracts and orders.

Subpart 1239.70—Information Security and Incident Response Reporting

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.

Subpart 1239.71—Protection of Data About Individuals

1239.7100 Scope of subpart.

This subpart includes Privacy Act and data protection considerations for DOT contracts. Data protection requirements are in addition to provisions concerning the general protection of individual privacy (*see* FAR subpart 24.1) and privacy in the acquisition of information technology (*see* FAR 39.105). DOT rules and regulations implementing the Privacy Act of 1974 are located at 49 CFR part 10.

1239.7101 Definitions.

As used in this subpart—

Breach means the disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized access, compromise, use, disclosure, modification, destruction, access or loss use of data, or the copying of information to unauthorized media may have occurred.

Data protection means the practice of protecting data and managing risks associated with the collection, display, use, processing, storage, transmission, and disposal of information or data as well as the systems and processes used for those purposes. Data protection uses physical, technical, and administrative controls to protect the integrity, availability, authenticity, non-repudiation, and confidentiality of data by incorporating protection, detection, and reaction capabilities. Data protection encompasses not only digital data, but also data in analog or physical form, and applies to data in transit as well as data at rest.

Information security means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) *Integrity,* which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(2) *Confidentiality,* which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) *Availability,* which means ensuring timely and reliable access to and use of information.

Personally Identifiable Information (PII) means the definition as set forth in FAR 24.101.

Privacy incident means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access to PII regardless of format.

1239.7102 Policy.

DOT must ensure that data protection is provided for information and information systems in accordance with current policies, procedures, and statutes, including:

(a) The Clinger-Cohen Act.

(b) The E-Government Act.

(c) Federal Information Systems Modernization Act.

(d) Federal Information Processing Standards.

(e) OMB Circular A–130, Managing Information as a Strategic Resource.

(f) 49 CFR part 10, Maintenance of and Access to Records Pertaining to Individuals.

(g) DOT Order 1351.18, Privacy Risk Management Policy.

(h) DOT Order 1351.19, PII Breach Notification Controls.

(i) DOT Order 1351.28, Records Management.

(j) DOT Order 1351.37, Departmental Cyber Security Policy.

1239.7103 Responsibilities.

(a) The contracting officer will include appropriate data protection requirements in all contracts and other acquisition-related documents for DOT information created, collected, displayed, used, processed, stored, transmitted, and disposed of by contractors.

(b) The contracting officer will ensure all contracts with contractors maintaining information systems containing PII contain the appropriate clauses as may be required by the Federal Acquisition Regulation (FAR) and other OMB and agency memorandums and directives, to ensure that PII under the control of the contractor is maintained in accordance with Federal law and DOT policy.

(c) The contracting officer and assigned contracting officer's representatives and program and

project managers will obtain contractual assurances from third parties working on official DOT business that third parties will protect PII in a manner consistent with the privacy practices of the Department during all phases of the system development lifecycle.

(d) Program and project managers and requiring activities will address the need to protect information about individuals and/or PII in the statement of work (SOW), performance work statement (PWS) or statement of objectives (SOO). Contracting officers will notify the appropriate organization or office when it intends to issue a solicitation for items or services requiring access to personal information or PII. Contracting officers will identify the Component Privacy Officer as the point of contact for oversight of privacy protection and identify the Component Information Systems Security Manager for the component for oversight of information security to the contractor after award.

(e) See 1252.239–75, DOT Protection of Information about Individuals, PII and Privacy Risk Management Requirements, for additional information regarding the requirements of DOT Order 1351.18, Privacy Risk Management Policy and DOT Order 1351.37, Departmental Cyber Security Policy.

1239.7104 Contract clause.

The contracting officer shall insert the clause at 1252.239–75, DOT Protection of Information About Individuals, PII and Privacy Risk Management Requirements, in solicitations and contracts involving contractor performance of data protection functions and for contracts involving the design, development, or operation of an information system with access to personally identifiable information as described in DOT Order 1351.18, Privacy Risk Management, and DOT Order 1351.37, Departmental Cyber Security Policy.

Subpart 1239.72—Cloud Computing

1239.7200 Scope of subpart.

This subpart prescribes policies and procedures for the acquisition of cloud computing services.

1239.7201 Definitions.

As used in this subpart—

Authorizing official means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Cloud computing means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.,* networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service,

broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

Government data means any information, document, media, or machine-readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

Government-related data means any information, document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. This does not include a contractor's business records (*e.g.,* financial records, legal records, and other similar records) or data such as operating procedures, software coding, or algorithms that are not uniquely applied to the Government data.

1239.7202 Policy.

(a) *General.* Generally, DOT entities shall acquire cloud computing services using commercial terms and conditions that are consistent with Federal law and the agency's needs, including those requirements specified in this subpart. Some examples of commercial terms and conditions are license agreements, End User License Agreements (EULAs), Terms of Service (TOS), or other similar legal instruments or agreements. Contracting officers shall carefully review commercial terms and conditions and consult counsel to ensure these are consistent with Federal law, regulations, and the agency's needs. Contracting officers shall incorporate any applicable service provider terms and conditions into the contract by attachment or other appropriate mechanism.

(b) *FedRAMP provisional authorization.* Except as provided in paragraph (b)

(1) of this section, the contracting officer shall only award a contract to acquire cloud computing services from a cloud service provider (*e.g.,* contractor or subcontractor, regardless of tier) that has been granted provisional authorization by the General Services Administration (GSA) Federal Risk and Authorization Management Program (FedRAMP), and meets the security requirements set out by the DOT Chief Information Officer (CIO), at the level appropriate to the requirement to provide the relevant cloud computing services.

(1) The contracting officer may award a contract to acquire cloud computing services from a cloud service provider that has not been granted provisional authorization when—

(i) The requirement for a provisional authorization is waived by the DOT CIO; or

(ii) The cloud computing service requirement is for a private, on-premises version that will be provided from Government facilities. Under this circumstance, the cloud service provider must obtain a provisional authorization prior to operational use.

(2) When contracting for cloud computing services, the contracting officer shall ensure the following information is provided by the requiring activity:

(i) Government data and Government-related data descriptions.

(ii) Data ownership, licensing, delivery, and disposition instructions specific to the relevant types of Government data and Government-related data (*e.g.,* Contract Data Requirements List; work statement task; line items). Disposition instructions shall provide for the transition of data in

commercially available, or open and non-proprietary format (and for permanent records, in accordance with disposition guidance issued by National Archives and Record Administration).

(iii) Appropriate requirements to support applicable inspection, audit, investigation, or other similar authorized activities specific to the relevant types of Government data and Government-related data, or specific to the type of cloud computing services being acquired.

(iv) Appropriate requirements to support and cooperate with applicable system-wide search and access capabilities for inspections, audits, investigations.

(c) *Required storage of data within the United States or outlying areas.*

(1) Cloud computing service providers are required to maintain within the 50 States, the District of Columbia, or outlying areas of the United States, all Government data that is not physically located on DOT premises, unless otherwise authorized by the DOT CIO.

(2) The contracting officer shall provide written approval to the contractor when the contractor is permitted to maintain Government data at a location outside the 50 States, the District of Columbia, and outlying areas of the United States.

1239.7203 DOT FedRAMP specific requirements.

DOT entities shall set forth DOT FedRAMP specific cloud service requirements. DOT cloud service providers shall adhere to specific requirements when providing services to DOT and its operating administrations whenever DOT or other Federal agency information, sensitive information as defined by DOT policy, personally identifiable information, or third-party provided information and data will transit through or reside on the cloud services system and infrastructure and that requires protection according to required National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS). In addition to the requirements found elsewhere in the FAR, the following are required—

(a) *Validated cryptography for secure communications.* The FedRAMP security control baseline requires cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (see NIST FIPS 140–2). DOT entities must require FIPS 140–2 validated cryptography be used between DOT and the cloud service provider. The program/project manager or requiring activity shall specify which level (1–4) of FIPS 140–2 validation is required. See the clause prescribed at 1239.7204(c).

(b) *Digital signature cryptography—(authentication, data integrity, and non-repudiation).* Cloud service providers are required to implement FIPS 140–2 validated cryptography for digital signatures. If DOT entities require integration with specific digital signature technologies, contracting officers shall specify what level (1–4) of FIPS 140–2 encryption is required. See the clause prescribed at 1239.7204(d).

(c) *Audit record retention for cloud service providers.* DOT entities should consider the length of time Cloud Service Providers (CSP) must retain audit records. DOT implements the FedRAMP requirement for a service provider to retain system audit records on-line for at least ninety calendar days and to further preserve audit records off-line for a period that is in accordance with DOT and NARA requirements. See the clause prescribed at 1239.7204(e).

(d) *Cloud identification and authentication (organizational users) multi-factor authentication.* Cloud

Service Providers pursuing a FedRAMP authorization must provide a mechanism for DOT activities and operating administrations (*i.e.,* Government consuming end-users) to use multi-factor authentication. DOT follows National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication (PUB) Number 201–2, Personal Identity Verification (PIV) of Federal Employees and Contractors. See the clause prescribed at 1239.7204(f).

(e) *Identification and authentication (non-organizational users).* Contracting officers shall require that Cloud Service Providers pursuing a FedRAMP authorization provide multi-factor authentication for the provider's administrators. See the clause prescribed at 1239.7204(g).

(f) *Incident reporting timeframes.* Contracting officers shall specify in solicitations and contracts the required FedRAMP parameters for Incident Reporting at the levels stipulated in NIST SP 800–61, as well as the requirement for an Incident Reporting Plan that complies with those requirements. The program office shall include specific incident reporting requirements including who and how to notify the agency. See 1239.7002(b) and the clause prescribed at 1239.7204(h).

(g) *Media transport.* DOT or other Federal agency information and data require protection. Contracting officers shall set forth specific DOT media transport requirements. See the clause prescribed at 1239.7204(i).

(h) *Personnel screening—background investigations.* When DOT leverages FedRAMP Provisional Authorizations, DOT conducts the required background investigations, but may accept reciprocity from other agencies that have implemented the Cloud Service Provider's systems. DOT's screening procedures, process, and additional screening requirements are set forth at 1252.204–70 and the clause prescribed at 1239.7204(j).

(i) *Minimum personnel security requirements—U.S. citizenship and clearance.* Contractors shall provide support personnel who are U.S. persons maintaining a NACI clearance or greater in accordance with OMB memoranda and contract clauses, and who shall undergo required DOT background investigations prior to providing services and performing on the contract. See clause 1252.204–70(b) and the clause prescribed at 1239.7204(j). Reinvestigations are required for cloud services provider personnel as follows—

(1) Moderate risk law enforcement and high impact public trust level—a reinvestigation is required during the 5th year; and

(2) There is no reinvestigation for other moderate risk positions or any low risk positions.

1239.7204 Contract clauses.

(a) The contracting officer shall insert the clause at 1252.239–76, Cloud Computing Services, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(b) The contracting officer shall insert a clause substantially as follows at 1252.239–77, Data Jurisdiction, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(c) The contracting officer shall insert a clause substantially as follows at 1252.239–78, Validated

Cryptography for Secure Communications, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(d) The contracting officer shall insert a clause substantially as follows at 1252.239–79, Authentication, Data Integrity, and Non-Repudiation, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(e) The contracting officer shall insert a clause substantially as follows at 1252.239–80, Audit Record Retention for Cloud Service Providers, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(f) The contracting officer shall insert a clause substantially as follows at 1252.239–81, Cloud Identification and Authentication (Organizational Users) Multi-Factor Authentication, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(g) The contracting officer shall insert a clause substantially as follows at 1252.239–82, Identification and Authentication (Non-Organizational Users), in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(h) The contracting officer shall insert a clause substantially as follows at 1252.239–83, Incident Reporting Timeframes, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(i) The contracting officer shall insert a clause substantially as follows at 1252.239–84, Media Transport, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(j) The contracting officer shall insert a clause substantially as follows at 1252.239–85, Personnel Screening—Background Investigations, in all services solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(k) The contracting officer shall insert a clause substantially as follows at 1252.239–86, Boundary Protection—Trusted Internet Connections, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(l) The contracting officer shall insert a clause substantially as follows at 1252.239–87, Protection of Information at Rest, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services involving cloud computing services.

(m) The contracting officer shall insert a clause substantially as follows at 1252.239–88, Security Alerts, Advisories, and Directives, in solicitations and contracts, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information

technology services involving cloud computing services.

Subpart 1239.73—Technology Modernization and Upgrades/Refreshment

1239.7300 Scope of subpart.

This subpart prescribes policies and procedures for incorporating technology modernization, upgrades, and refreshment into acquisitions involving information technology products or services supporting the development of applications, information systems, or system software.

1239.7301 Definitions.

As used in this subpart—

Application means the software that resides above system software and includes applications such as database programs, word processors and spreadsheets. Application software may be bundled with system software or published alone.

Modernization means the conversion, rewriting or porting of a legacy system to a modern computer programming language, software libraries, protocols, or hardware platform.

Refresh means the periodic replacement of equipment to ensure continuing reliability of equipment and/or improved speed and capacity.

System software means a platform composed of operating system programs and services, including settings and preferences, file libraries and functions used for system applications. System software also includes device drivers that run basic computer hardware and peripherals.

Upgrade means an updated version of existing hardware, software or firmware. The purpose of an upgrade is improved and updated product features, including performance, product life, usefulness and convenience.

1239.7302 Policy.

Contracting officers will ensure all documents involving the acquisition of development or maintenance of DOT applications, systems, infrastructure, and services contain the appropriate clauses as may be required by the Federal Acquisition Regulation (FAR) and other Federal authorities, in order to ensure that information system modernization is prioritized accordance with Federal law, OMB Guidance, and DOT policy.

1239.7303 Contract clauses.

(a) The contracting officer shall insert the clause at 1252.239–89, Technology Modernization, in solicitations and contracts when the contractor or a subcontractor, at any tier, proposes a

modernization approach to develop or maintain information systems, applications, infrastructure, or services.

(b) The contracting officer shall insert the clause at 1252.239–90, Technology Upgrades/Refreshment, in solicitations and contracts when the contractor or a subcontractor at any tier, proposes technology improvements (upgrades/refreshments) to develop or maintain information systems, applications, infrastructure, or services.

Subpart 1239.74—Records Management

1239.7400 Scope of subpart.

This subpart prescribes policies for records management requirements for contractors who create, work with, or otherwise handle Federal records, regardless of the medium in which the records exist.

1239.7401 Definition.

As used in this subpart—

Federal record, as defined in 44 U.S.C. 3301, means 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.

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

1239.7402 Policy.

(a) *Requirements—*

(1) *Compliance.* Contractors shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to 44 U.S.C. chapters 21, 29, 31, and 33, NARA regulations at 36 CFR chapter XII, subchapter B, and those policies associated with the safeguarding of records covered by Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

(2) *Applicability.* In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended, and must be managed and scheduled for disposition only as permitted by relevant records management laws and regulations and DOT Order 1351.28, Departmental Records Management Policy.

(3) *Records maintenance.* While DOT records are in a contractor's custody, the contractor is responsible for preventing the alienation or unauthorized destruction of the DOT records, including all forms of mutilation. Records may not be removed from the legal custody of DOT or destroyed except in accordance with the provisions of the agency records schedules and with the written concurrence of the DOT or Component Records Officer, as appropriate. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, the contractor must report the event to the contracting officer, in accordance with 36 CFR part 1230, for reporting to NARA.

(4) *Unauthorized disclosure.* Contractors shall notify the contracting officer within two hours of discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Contractors shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of the information, data, documentary material, records and/or equipment accessed, maintained, or created. Contractors shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the contracting officer or contracting officer's representative. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to DOT control or the contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the contracting officer or address prescribed in the contract. Destruction of records is expressly prohibited unless authorized.

(b) *Non-public information.* Contractors shall not create or maintain any records containing any non-public DOT information that are not specifically tied to or authorized by the contract.

1239.7403 Contract clause.

The contracting officer shall insert the clause at 1239.239–91, Records Management, in all solicitations and contracts involving services where contractors or subcontractors and their employees or associates collect, access, maintain, use, disseminate, or otherwise handle Federal records.