Subpart 1239.72—Cloud Computing

Parent topic: PART 1239—ACQUISITION OF INFORMATION TECHNOLOGY

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.