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.

Parent topic: Subpart 1239.72—Cloud Computing