1252.239-76 Cloud Computing Services.

As prescribed in 1239.7204(a), insert the following clause:

CLOUD COMPUTING SERVICES (DATE)

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

Authorizing official, as described in Appendix B of DOT Order 1350.37, Departmental Cybersecurity Policy, means the senior Federal official or executive with the 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.

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.

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.

Government data means any information, document, media, or 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 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 contractor's business records *e.g.,* financial records, legal records etc. or data such as operating procedures, software coding, or algorithms that are not uniquely applied to the Government data.

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

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.

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

(b) *Cloud computing security requirements*. The requirements of this clause are applicable when using cloud computing to provide information technology services in the performance of the contract.

(1) If the Contractor indicated in its offer that it does not anticipate the use of cloud computing services in the performance of a resultant contract, and after the award of this contract, the Contractor proposes to use cloud computing services in the performance of the contract, the Contractor shall

obtain approval from the Contracting Officer prior to utilizing cloud computing services in performance of the contract.

(2) The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the DOT Order 1351.37, Departmental Cybersecurity Policy, and the requirements of DOT Order 1351.18, Departmental Privacy Risk Management Policy (the versions of each that in effect at the time the solicitation is issued or as authorized by the Contracting Officer), unless notified by the Contracting Officer that this requirement has been waived by the DOT Chief Information Officer.

(3) The Contractor shall maintain all Government data not physically located on DOT premises within the United States, the District of Columbia, and all territories and possessions of the United States, unless the Contractor receives written notification from the Contracting Officer to use another location, in accordance with DOT Policy.

(4) DOT will determine the security classification level for the cloud system in accordance with Federal Information Processing Standard 199; the Contractor will then apply the appropriate set of impact baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance with security standards. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, Security Control Baselines and also includes a set of additional controls for use within systems providing cloud services to the Federal government.

(5) The Contractor shall maintain a security management continuous monitoring environment that meets or exceeds the requirements in the Reporting and Continuous Monitoring section of this contract/task order _____ [*Fill-in: Contracting Officer enter the requirements document paragraph reference number*] based upon the latest edition of FedRAMP

Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements.

(6) The Contractor shall be responsible for the following privacy and security safeguards:

(i) To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall provide the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(ii) The Contractor shall also comply with any additional FedRAMP and DOT Orders containing cybersecurity and privacy policies.

(7) The Government may perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisition Regulation (FAR) clause 52.239-1, Privacy or Security Safeguards, the Contractor shall provide the Government access to Contractor's facilities, installations, technical capabilities, operations, documentation, records and databases to carry out a program of inspection. Contractors shall provide access within two hours of notification by the Government. The program of inspection shall include, but is not limited to—

(i) Authenticated and unauthenticated operating system/network vulnerability; scans;

(ii) Authenticated and unauthenticated web application vulnerability scans;

(iii) Authenticated and unauthenticated database application vulnerability scans; and

(8) Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

(9) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(10) If the vendor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, the Government will approve scanning tools and their configuration. In addition, the Contractor shall provide complete results of vendor-conducted scans to the Government.

(c) *Limitations on access to and use and disclosure of Government data and Government-related data.*

(1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order or delivery order issued hereunder.

(i) If authorized by the terms of this contract or a task order or delivery order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order or delivery order.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of this contract.

(2) The Contractor shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(d) *Cloud computing services cyber incident reporting*. The Contractor shall report all cyber incidents related to the cloud computing service provided under this contract. 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 2 hours of discovery.

(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 agency procedures.

(f) *Malicious software*. The Contractor or subcontractor(s) that discovers and isolates malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by 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 the cyber incident report (*see* paragraph 5 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 7 of this clause.

(j) *Subcontract flowdown requirement*. The Contractor shall include this clause, including this paragraph (j), in all subcontracts that involve or may involve cloud services, including subcontracts for commercial products or commercial services.

(End of clause)

1252.239-77 Data Jurisdiction.

As prescribed in 1239.7204(b), insert a clause substantially as follows:

DATA JURISDICTION (DATE)

The Contractor shall identify all data centers in which the data at rest or data backup will reside, including primary and replicated storage. The Contractor shall ensure that all data centers not physically located on DOT premises reside within the United States, the District of Columbia, and all territories and possessions of the United States, unless otherwise authorized by the DOT CIO. The Contractor shall provide a Wide Area Network (WAN), with a minimum of _____ [*Contracting Officer fill-in: Insert specific number*] data center facilities at _____ [*Contracting Officer fill-in number*] different geographic locations with at least _____ [*Contracting Officer fill-in number*] Internet Exchange Point (IXP) for each price offering. The Contractor shall provide Internet bandwidth at the minimum of _____ [*Contracting Officer fill-in applicable gigabytes*] GB.

(End of clause)

1252.239-80 Audit Record Retention for Cloud Service Providers.

As prescribed in 1239.7204(e), insert the following clause:

AUDIT RECORD RETENTION FOR CLOUD SERVICE PROVIDERS (DATE)

(a) The Contractor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with 36 CFR 1236.20 and 1236.22, including but not limited to capabilities such as those identified in DoD STD-5015.2 V3, Electronic Records Management Software Applications Design Criteria Standard, NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving applications to store e-mail, and NARA Bulletin 2010-05 September 08, 2010, Guidance on Managing Records in Cloud Computing Environments.

(b) The Contractor shall maintain records to retain functionality and integrity throughout the records' full lifecycle including—

(1) Maintenance of links between records and metadata; and

(2) Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA approved retention schedules.

(End of clause)

1252.239-83 Incident Reporting Timeframes.

As prescribed in 1239.7204(h), insert the following clause:

INCIDENT REPORTING TIMEFRAMES (DATE)

(a) The Contractor shall report all computer security incidents to the DOT Security Operations Center (SOC) in accordance with Subpart 1239.70—Information Security and Incident Response Reporting.

(b) Contractors and subcontractors are required to report cyber incidents directly to DOT via the DOT 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 2 hours of discovery, regardless of the incident category. See 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting.

(End of clause)

1252.239-85 Personnel Screening—Background Investigations.

As prescribed in 1239.7204(j), insert the clause as follows:

PERSONNEL SCREENING—BACKGROUND INVESTIGATIONS (DATE)

(a) Contractors shall provide support personnel who are U.S. persons maintaining a NACI clearance or greater in accordance with OMB memorandum M-05-24, Section C. (*see* https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2005/m05-24.pdf.

(b) The Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel supporting the system. The Contractor shall also comply with Executive Order 12968, Access to Classified Information. DOT separates the risk levels for personnel working on Federal computer systems into three categories: low risk,

moderate risk, and high risk. The Contractor is responsible for the cost of meeting all security requirements and maintaining assessment and authorization.

(c) The Contractor's employees with access to DOT systems containing sensitive information may be required to obtain security clearances (*i.e.*, Confidential, Secret, or Top Secret). National Security work designated "special sensitive," "critical sensitive," or "non-critical sensitive," will determine the level of clearance required for contractor employees. Personnel security clearances for national security contracts in DOT will be processed according to the Department of Defense National Industrial Security Program Operating Manual (NISPOM).

(d) The Contracting Officer, through the Contracting Officer's Representative (COR) or Program Manager will ensure that all required information is forwarded to the Federal Protective Service (FPS) in accordance with the DOT Policy. FPS will then contact each Applicant with instructions for completing required forms and releases for the type of personnel investigation requested.

(e) Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS, OPM or DoD, there has been no break in service, and the position is identified at the same or lower risk level. Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a DOT identity credential (if required) and initial access to information systems holding DOT information.

(End of clause)

1252.239-88 Security Alerts, Advisories, and Directives.

As prescribed in 1239.7204(m), insert the clause as follows:

SECURITY ALERTS, ADVISORIES, AND DIRECTIVES (DATE)

The Contractor shall provide a list of its personnel, identified by name and role, who are assigned system administration, monitoring, and/or security responsibilities and who are designated to receive security alerts, advisories, and directives and individuals responsible for the implementation of remedial actions associated with them.

(End of clause)