U.S. Department of Transportation

1200 New Jersey Ave., S.E.
Washington, DC 20590

Office of the Secretary of Transportation

SUBJECT: Class Deviation No. 2026-39 from the Transportation Acquisition Regulation for TAR Part 1239 in Support of Executive Order 14275, Restoring Common Sense to Federal Procurement

FROM: Chrishaun Jones
Senior Procurement Executive
Office of the Senior Procurement Executive

CHRISHAUN PATRICE JONES
Digitally signed by CHRISHAUN PATRICE JONES
Date: 2026.10.28 00:05:45 -04'00'

TO: Department of Transportation Chiefs of the Contracting Offices

I. Purpose: This memorandum approves a class deviation to the Transportation Acquisition Regulation (TAR) part 1239 for the purpose of implementing, in the TAR, Federal Acquisition Regulation (FAR) Class Deviation (CD) (No. 2025-07) for FAR part 39 in support of Executive Order (E.O.) 14275, "Restoring Common Sense to Federal Procurement."

II. Effective Date: 1 December 2026.

III. Background: On April 15, 2025, Executive Order (E.O.) 14275, Restoring Common Sense to Federal Procurement was signed. Section 2 of the E.O. establishes the policy that the FAR "should only contain provisions required by statute or essential to sound procurement, and any FAR provisions that do not advance these objectives should be removed." The Revolutionary FAR Overhaul (RFO) initiative will make the FAR more concise, understandable, and focused on core procurement requirements. This also applies to agency supplements to the FAR.

Under this initiative, the FAR is being updated to:

- Remove language that is not required by statute
- Remove duplicative or outdated language
- Clarify or provide more plain language
- Revise language for the new FAR framework
- Retain language necessary for governmentwide acquisition standards.

The RFO FAR part 39 model deviation text upon which this RFO TAR part 1239 deviation is based, establishes bedrock principles. The Department of Transportation (DOT) issued FAR CD 2025-07 for FAR part 39 on July 2, 2025.

DOT also issued TAR Class Deviation 2024-02 - Transportation Acquisition Regulation (TAR) Class Deviation (CD) – TAR 1202.101, 1239.7103(f), 1245.102-70, 1245.107-70, and 1252.245-70 on March 29, 2024, concerning use of Government Furnished Equipment/Information and prohibition on access while on international travel.

To ensure alignment with issued E.O.s and the RFO FAR part CD, it is necessary to issue this RFO TAR CD in advance of a proposed rule to implement these requirements to ensure DOT policies and procedures align with these requirements. DOT intends on conducting further analysis and developing a rule for publication in the Federal Register for public comment after the release of this CD, and after FAR proposed and final rules are published.

IV. Summary of Changes: The following table is not an exhaustive list but includes notable updates to TAR part 1239:

Change	Description

New/Retained/ Updated	General – Retained as the coverage directly implements a specific statute. Updated TAR content and headings to align with RFO FAR Part 39.
	
	• **1239.001, Applicability.** New.
	  o Contains previous content from "Scope of part" to align with RFO FAR part 39 treatment.
	  o Slight revisions to remove express "cloud computing" content now placed in TAM Part 1239 and Appendix A as internal agency guidance for including in statements of work (SOWs), performance work statements (PWS's), and other requirements documents.
	
	Subpart 1239.1—Presolicitation. New. Aligns with new RFO FAR part 39 title from previous "General."
	• **1239.170, Policy.** Moved from 1239.101-73. **Revised to point to TAM Part 1239, Appendix A for requirements terms and conditions (T&Cs)** where certain TAR solicitation provisions and contract clauses are now moved to Appendix A as shown below, and which are to be included in SOWs, PWS's, and other requirements documents.
	• **1239.171, Contract clauses.** (From previous 1239.106-70.
	  o Retains prescriptions for clauses 1252.239-70, 1252.239-74, 1252.239-75, and 1252.239-93 (as noted in detail below).
	Subpart 1239.3—Postaward. New. Adds TAR subpart to align with new RFO FAR part 39 subpart.
	• **1239.370, Safeguarding DOT Data and Reporting of Cyber Incidents.**
	  o Retains and moves critical breach and cyber security reporting incidents requirements during contract performance.
	• **1239.371, Accessing DOT Data or Systems Outside U.S. and Use of Government Furnished Equipment.** New.
	  o Moves content from previous TAR CD 2024-02 to better align with IT and information system prohibitions concerning use of DOT IT equipment and access to DOT systems.

	o Outlines requirement for prior approval in accordance with OCDIO procedures. • **1239.372, Contract clause.** New. o Prescribes clause 1252.239-94, Use of Government Furnished Equipment or Information—Official, Unofficial, and Personal International Travel, in solicitations and contracts where government furnished property is provided or access to Government data and information systems is required in the performance of services. **Subpart 1239.70—Technology Modernization, Upgrades and Refreshment.** • Redesignated and retitled from previous Subpart 1239.73, Technology Modernization, and Upgrades/Refreshment. • 1239.7000, Scope of subpart. Renumbered/redesignated. • 1239.7001, Contract clause. Renumbered/redesignated and updated the prescription. Combined and streamlined the two previous provision and clause into one clause: 1252.239-89, Technology Modernization, Upgrades and Refreshment. **Subpart 1239.71—Records Management.** Revised number/designation. • Moved content from existing subpart 1239.74; retained with minimal revisions. The following sections retained, but renumbered/redesignated: o 1239.7100, Scope of subpart. o 1239.7101, Definition. o 1239.7102, Policy. o 1239.7103, Contract clause. Prescribes clause TAR 1239.239-91, Records Management. Retains and updates the following provisions and clauses to align with the RFO FAR part, updates citations, and retains current clause or provision numbering; removes non-regulatory content to the TAM or TAM, Appendix A (including certain provisions and clauses shown as "Removed" below in the second block): • **1252.239-70, Security Requirements for Unclassified Information Technology Resources.** (DEC 2026)(RFO DEVIATION). o Streamlined per RFO FAR drafting guidelines; moved content more appropriate to SOWs, PWS's, and other requirements documents to TAM Part 1239, Appendix A, as numbered requirements terms and conditions (T&Cs) - TC 1239.01). • **1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting.** (DEC 2026)(RFO DEVIATION). o Streamlined per RFO FAR drafting guidelines; moved content more appropriate to SOWs, PWS's, and other requirements documents to TAM Part 1239, Appendix A, as numbered requirements terms and conditions (T&Cs) - TC 1239.05). o Retained content on Cyber incident reporting and cyber incident damage assessment activities, and subcontract flowdown requirements.

	• **1252.239-75, DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements.** (DEC 2026)(RFO DEVIATION) o Retained most text; slightly revised to reflect RFO FAR drafting guidelines. o Streamlined per RFO FAR drafting guidelines; moved content more appropriate to SOWs, PWS's, and other requirements documents to TAM Part 1239, Appendix A, as numbered requirements terms and conditions (T&Cs) - TC 1239.06 on reporting breaches as the reporting requirement is also reflected in TAR clause 1252.239-74. • **1252.239-89, Technology Modernization, Upgrades and Refreshment.** (DEC 2026) (RFO DEVIATION). o Combined with 1252.239-90; streamlined to align with RFO FAR drafting guidelines. Created one clause; eliminated one provision. • **1252.239-91, Records Management.** (DEC 2026)(RFO DEVIATION) o Retained most of text; slightly revised to reflect RFO FAR format and drafting style. • **1252.239-93, Information and Communication Technology Accessibility**. (DEC 2026) (RFO DEVIATION). o Combined and streamlined the original provision at 1252.239-92 with this -93 clause. o Streamlined per RFO FAR drafting guidelines; moved content more appropriate to SOWs, PWS's, and other requirements documents to TAM Part 1239, Appendix A, as numbered requirements terms and conditions (T&Cs) - TC 1239.21). • **1252.239-94, Use of Government Furnished Equipment or Information —Official, Unofficial, and Personal International Travel.** (DEC 2026)(RFO DEVIATION). o Moved this clause from a previous TAR CD now rescinded with this CD issuance. Streamlined per RFO FAR drafting guidelines.
Removed	General – Text has been revised/deleted in the subpart/section below to remove non-statutory guidance. Moved content from the TAR to the TAM, Appendix A, including some solicitation provisions and contract clauses as described below which were prescribed for inserting into agency statements of work (SOWs), performance work statements (PWS's), and other requirements documents. This aligns with the RFO FAR and drafting principles, as well as GSA and other civilian agency approaches on incorporating certain ICT and related requirements into SOWs, PWS's, and other requirements documents. • 1239.000 Scope of part. No RFO FAR part. Content now at 1239.001. • 1239.002 Definitions. No RFO FAR part. Unnecessary. **Subpart 1239.1—General.** Removed. • Subpart renumbered to align with RFO FAR Part 39. • Underlying sections moved to internal agency guidance: o 1239.101-70, Policy—software management and development. o 1239.101-71, Scope.

	o 1239.101-72, Definitions. o 1239.101-73, Policy. **Subpart 1239.2—Information and Communication Technology.** • Removed. No RFO FAR subpart. Coverage now in internal agency policy. Contract clauses combined and now prescribed at at 1239.171 under TAR subpart 1239.1—Presolicitation. • Underlying sections moved to internal agency guidance: o 1239.201 Scope of subpart. o 1239.203 Applicability. **Subpart 1239.70—Information Security and Incident Response Reporting** • Removed. No RFO FAR subpart. Coverage now in internal agency policy and at new RFO TAR subpart 1239.3—Postaward. • Underlying sections moved to internal agency guidance and to subpart 1239.3: o 1239.7000, Scope of subpart. o 1239.7001, Definitions. o 1239.7002, Policy. o 1239.7003, Contract clauses. **Subpart 1239.71—Protection of Data About Individuals** • Removed. No RFO FAR subpart. Coverage now in internal agency policy. • Underlying sections moved to internal agency guidance and TAM Part 1239, Appendix A for inclusion in SOWs, PWS's, and other requirements documents: o 1239.7100, Scope of subpart. o 1239.7101, Definitions. o 1239.7102, Policy. o 1239.7103, Responsibilities. o 1239.7104, Contract clause. **Subpart 1239.72—Cloud Computing** • Removed. No RFO FAR subpart. Coverage now in internal agency policy. • Underlying sections moved to internal agency guidance and TAM Part 1239, Appendix A for inclusion in SOWs, PWS's, and other requirements documents: o 1239.7200, Scope of subpart. o 1239.7201, Definitions. o 1239.7202, Policy. o 1239.7203, DOT FedRAMP specific requirements. o 1239.7204, Contract clauses. **Subpart 1239.73—Technology Modernization and Upgrades/Refreshment.**

	• Redesignated and retitled as Subpart 1239.70, Tcehnology Modernization, Upgrades, and Refreshment.
	• Underlying sections moved to internal agency guidance and TAM Part 1239, Appendix A for inclusion in SOWs, PWS's, and other requirements documents:
	  o 1239.7301, Definitions.
	  o 1239.7302, Policy
	
	Removed the following solicitation provisions and contract clauses. Most placed in the TAM Part 1239, Appendix A – Requirements Terms and Conditions (T&Cs) for inclusion in solicitation and contract SOWs, PWS's and other requirements documents, or were combined into one clause, as noted:
	
	• 1252.239-71, Information Technology Security Plan and Accreditation. (NOV 2022)
	• 1252.239-72, Compliance with Safeguarding DOT Sensitive Data Controls. (NOV 2022)
	• 1252.239-73, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. (NOV 2022)
	• 1252.239-76, Cloud Computing Services. (NOV 2022)
	• 1252.239-77, Data Jurisdiction. (NOV 2022)
	• 1252.239-78, Validated Cryptography for Secure Communications. (NOV 2022)
	• 1252.239-79, Authentication, Data Integrity, and Non-Repudiation. (NOV 2022)
	• 1252.239-80, Audit Record Retention for Cloud Service Providers. (NOV 2022)
	• 1252.239-81, Cloud Identification and Authentication (Organizational Users) Multi-Factor Authentication. (NOV 2022)
	• 1252.239-82, Identification and Authentication (Non-Organizational Users). (NOV 2022)
	• 1252.239-83, Incident Reporting Timeframes. (NOV 2022)
	• 1252.239-84, Media Transport. (NOV 2022)
	• 1252.239-85, Personnel Screening—Background Investigations. (NOV 2022)
	• 1252.239-86, Boundary Protection—Trusted Internet Connections. (NOV 2022)
	• 1252.239-87, Protection of Information at Rest. (NOV 2022)
	• 1252.239-88, Security Alerts, Advisories, and Directives. (NOV 2022)
	• 1252.239-90, Technology Upgrades/Refreshment. (NOV 2022)
	• 1252.239-92, Information and Communication Technology Accessibility Notice. (NOV 2022)

V. **Required Actions:** Contracting Officers shall follow the RFO TAR part 1239 deviation text, including the corresponding part 1252 deviation text, in lieu of TAR part 1239 and part 1252 as codified at 48 CFR, chapter 12. The RFO TAR deviation text is shown in the Attachment including any cognizant TAR part 1252 solicitation provisions or contract clauses prescribed in TAR part 1239.

Chiefs of the Contracting Offices (COCOs) must ensure this deviation is disseminated to the acquisition workforce and ensure compliance with the requirements in the CD.

For new solicitations, contracts or orders:

- Include applicable deviated provisions and clauses (marked **(DEC 2026)(RFO Deviation)**) as attached.
- For removed clauses 1252.239-71, 1252.239-72, 1252.239-73, 1252.239-76, 1252.239-77, 1252.239-78, 1252.239-79, 1252.239-80, 1252.239-81, 1252.239-82, 1252.239-83, 1252.239-84, 1252.239-85, 1252.239-86, 1252.239-87, 1252.239-88, 1252.239-89, 1252.239-90, and 1252.239-92, the text is now moved in the interim to a **TAM Note 2026-02, Appendix A** that requires the text (newly numbered requirements terms and conditions (T&Cs) in the TAM Note) in contract SOWs, PWS's, and other requirements documents pending any updated guidance from the Office of the Chief Digital & Information Officer (OCDIO).
- See **TAM Note 2026-02** issued this same date and effective 1 December 2026. Include the applicable TAM Part 1239, Appendix A – Requirements Terms and Conditions (T&Cs).

For open solicitations:

- The contracting officer has discretion regarding the need to enforce or amend the provisions or clauses. Note that without some of the removed provisions or clauses, the contracting officer may be required to separately address certain aspects in an awarded contract.

For existing contracts and orders:

- No action required for the clause associated with this class deviation.

Rescind existing TAR CD 2024-02 based on issuance of this TAR CD 2026-39:

- TAR Class Deviation 2024-02 - Transportation Acquisition Regulation (TAR) Class Deviation (CD) – TAR 1202.101, 1239.7103(f), 1245.102-70, 1245.107-70, and 1252.245-70 on March 29, 2024, concerning use of Government Furnished Equipment/Information and prohibition on access while on international travel,is now fully rescinded because of this CD issuance, effective December 1, 2026.

VI. **Applicability:** This CD applies to all DOT Operating Administrations (OAs), the Office of the Secretary of Transportation (OST), and the Office of the Inspector General (OIG), excluding the Federal Aviation Administration (FAA) in accordance with RFO TAR 1201.103-70(b).

VII. **Authority:** This CD is issued under the authority of RFO FAR 1.304, Class deviations; TAR 1201.404, Class deviations; and the revised citation at RFO TAR 1201.304, for the purpose of implementing policy in the TAR to comply with requirements of certain E.O.s, statutes, and other directives in DOT FAR CD No. 2025-07.

VIII. **Expiration Date:** This CD will remain in effect until it is incorporated into the TAR, superseded, or is otherwise rescinded, whichever occurs first.

IX. **Point of Contact:** Questions or comments regarding this deviation may be directed to DOTAcquisitionPolicy@dot.gov.

Attachment:

A. RFO TAR Part 1239 & Applicable Part 1252 Deviation Text – Bold/Bracketed/Line-in Line-Out (BB-LILO)

Transportation Acquisition Regulation (TAR) Class Deviation (CD) No. 2026-39

Attachment A

RFO TAR Part 1239 and 1252 Deviation Text

TAR Text Baseline is 48 CFR chapter 12 as of August 12, 2026.

Additions are shown as **[bolded and bracketed]** and deletions are shown in strikethrough ~~deletions~~. TAR Text unchanged shown as asterisks.

*****

PART 1239—ACQUISITION OF INFORMATION [AND COMMUNICATION] TECHNOLOGY [(RFO Deviation)]

~~1239.000 Scope of part.~~
~~1239.002 Definitions.~~
[1239.001 Applicability.]

Subpart 1239.1—~~General~~[Presolicitation]
1239.**[71]**~~101~~ Policy.
~~1239.101-70 Policy—software management and development.~~
~~1239.101-71 Scope.~~
~~1239.101-72 Definitions.~~
~~1239.101-73 Policy.~~
1239.1**[71]**~~06-70~~ 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 1239.7[0]~~3~~—Technology Modernization and Upgrades/Refreshment
1239.7**[0]**~~3~~00 Scope of subpart.
~~1239.7301 Definitions.~~
~~1239.7302 Policy.~~
1239.7**[001]**~~303~~ Contract clause.

Subpart 1239.7[1]~~4~~—Records Management
1239.7**[1]**00 Scope of subpart.
1239.7**[1]**01 Definition.
1239.7**[1]**02 Policy.
1239.7**[1]**03 Contract clause.

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

PART 1239—ACQUISITION OF INFORMATION [AND COMMUNICATION] TECHNOLOGY [(RFO DEVIATION)]

~~**1239.000 Scope of part.**~~

[1239.001 Applicability.]

~~In addition to FAR 39.000, t~~

[(a)(1)] [T]his part prescribes ~~acquisition~~ policies and procedures for **[the following—]**~~use in acquiring information technology and information technology-related supplies, services and systems, including information security, to include—~~

~~(a) Software management and development~~**;[(i) ICT and services Federal and other policy requirements;]**

(**[ii]**~~b~~) Section 508 standards and compliance for contracts;

(**[iii]**~~c~~) Information security and incident response reporting;

(**[iv]**~~d~~) Protection of data about individuals;

~~(e) Cloud computing;~~

(**[v]**~~f~~) Technology modernization and upgrade/refreshment; and

(**[vi]**~~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~~[Presolicitation]

~~**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.~~

1239.1[70]~~01-73~~ Policy.

~~The contracting officer will ensure all documents involving t~~**[T]**he acquisition of products or services supporting the development or maintenance of **[DOT information and communication technology (ICT) and]** DOT software applications, systems, infrastructure, and services **[must]** contain ~~the~~ appropriate [solicitation provisions and contract clauses, and ~~clauses~~[**requirements terms and conditions]** as ~~may be~~ required by **[the]** Federal Acquisition Regulation (FAR)[, the TAR,] ~~and other~~ Federal ~~authorities~~**[statutes]**, ~~in order to ensure that information system modernization is prioritized accordance with Federal law,~~ OMB ~~Guidance,~~ **[and other Federal policies and guidance,]** and DOT policy. **[See TAM Note 2026-02, TAM Part 1239 and Appendix A (DEC 2026), Information and Communications Technology (ITC); and Information, Information Systems, and Related Services for requirements terms and conditions (T&Cs) applicable to solicitation and contracts statements of work, performance work statements, and other requirements documents.]**

1239.1[71]~~06-70~~ Contract clauses.

[(a)] ~~The contracting officer shall :~~ **[I]**nsert 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 **[ICT]** ~~information technology services~~.

[(b) Insert the 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.

(c) 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.

(d) Insert the clause at 1252.239-93, Information and Communication Technology Accessibility, in all contracts and orders.]

[Subpart 1239.3—Postaward

1239.370 Safeguarding DOT Data and Reporting of Cyber Incidents.

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. 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 in accordance with clause 1252.239-74 and the contract statement of work / requirements documents.

1239.371 Accessing DOT Data or Systems Outside U.S. and Use of Government Furnished Equipment.

(a) Contractors shall not use personal equipment to access DOT data or systems while outside the United States or its territories, whether on personal or official travel.

(b) Contractors shall obtain prior approval in accordance with OCDIO procedures for use of GFE to conduct DOT business or access DOT systems while outside the United States or its territories.

(c) Use of GFE outside the United States or its territories is only permitted if the contractor has received prior authorization for official DOT international travel and approval for the

use of DOT standard GFE from the Office of the Chief Digital and Information Officer (OCDIO), regardless of the destination country.

1239.372 Contract clause.

Insert the clause at 1252.239-94, Use of Government Furnished Equipment or Information—Official, Unofficial, and Personal International Travel, in solicitations and contracts where government furnished property is provided or access to Government data and information systems is required in the performance of 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.~~

~~(f) Contracting officers and program/project management offices shall ensure contractors are aware of and will implement the clause as prescribed at 1245.107-70, 1252.245-70, Use of Government Furnished Equipment or Information – Unofficial and Personal Travel Abroad. This shall be addressed at the time of post-award contract orientation for contractors providing services under any DOT issued contract where GFE or GFI is provided and accessed by contractor or subcontractor personnel.~~

~~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 1239.7[0]~~3~~—Technology Modernization[,] ~~and~~ Upgrades~~/~~[, and] Refreshment

1239.7[000]~~300~~ 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.~~

1239.7[001]~~303~~ Contract clause.

~~(a) The contracting officer shall i~~**[I]**nsert the clause at 1252.239-89, Technology Modernization **[and Upgrades/Refreshment]**, 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 1239.7[1]~~4~~—Records Management

1239.7[100]~~400~~ 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.

1239.7[101]~~401~~ 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.

1239.7[102]~~402~~ 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~~**[must]** 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~~**[must]** 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~~**[may]** 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~~**[must**] be returned to DOT control or the contractor must hold it until otherwise directed. Items returned to the Government ~~shall~~ **[may]** 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~~**[must**] not create or maintain any records containing any non-public DOT information that are not specifically tied to or authorized by the contract.

1239.7[103]~~403~~ Contract clause.

~~The contracting officer shall i~~**[I]**nsert 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.

Part 1252 – Solicitation Provisions and Contract Clauses (RFO Deviation)

Subpart 1252.2—Text of Provisions and Clauses

*** * * * ***

1252.239-70 Security Requirements for Unclassified Information Technology Resources. **[(DEC 2026)(RFO DEVIATION)]**

1252.239-71 ~~Information Technology Security Plan and Accreditation.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-72 ~~Compliance with Safeguarding DOT Sensitive Data Controls.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-73 ~~Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-74 Safeguarding DOT Sensitive Data and Cyber Incident Reporting. **[(DEC 2026)(RFO DEVIATION)]**

1252.239-75 DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements. **[(DEC 2026)(RFO DEVIATION)]**

1252.239-76 ~~Cloud Computing Services.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-77 ~~Data Jurisdiction.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-78 ~~Validated Cryptography for Secure Communications.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-79 ~~Authentication, Data Integrity, and Non-Repudiation.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-80 ~~Audit Record Retention for Cloud Service Providers.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-81 ~~Cloud Identification and Authentication (Organizational Users) Multi-Factor Authentication.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-82 ~~Identification and Authentication (Non-Organizational Users).~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-83 ~~Incident Reporting Timeframes.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-84 ~~Media Transport.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-85 ~~Personnel Screening—Background Investigations.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-86 ~~Boundary Protection—Trusted Internet Connections.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-87 ~~Protection of Information at Rest.~~ **[RESERVED] [(DEC 2026) (RFO DEVIATION)]**

1252.239-88 ~~Security Alerts, Advisories, and Directives.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-89 Technology Modernization **[and Upgrades/Refreshment]**. **[(DEC 2026)(RFO DEVIATION)]**

1252.239-90 ~~Technology Upgrades/Refreshment.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-91 Records Management. **[(DEC 2026)(RFO DEVIATION)]**

1252.239-92 ~~Information and Communication Technology Accessibility Notice.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

1252.239-93 ~~Information and Communication Technology Accessibility.~~ **[RESERVED] [(DEC 2026)(RFO DEVIATION)]**

[1252.239-94 Use of Government Furnished Equipment or Information —Official, Unofficial, and Personal International Travel.] [(DEC 2026)(RFO DEVIATION)]

*** * * * ***

Subpart 1252.2—Text of Provisions and Clauses

*** * * * ***

1252.239-70 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 1239.~~106-70~~**[171(a)],** insert the following clause:

Security Requirements for Unclassified Information Technology Resources (~~NOV 2022~~[DEC 2026]) [(RFO DEVIATION)]

(a) The Contractor ~~shall be~~ **[is]** responsible for information technology security for all systems connected to a Department of Transportation (DOT) network or operated by the Contractor for DOT, regardless of location. This ~~clause is applicable~~ **[applies]** to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to DOT information ~~that directly supports the mission of DOT~~. ~~The term "information technology," as used in this clause, means any equipment or interconnected system or subsystem of equipment, including telecommunications equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.~~ **[The Contractor shall comply with requirements set forth in the statement of work, performance work statement, and other requirements documents, and required directives at TAM Part 1239, Appendix A (DEC 2026): Information and Communications Technology (ITC); and Information, Information Systems, and Related Services for requirements terms and conditions (T&Cs) applicable to solicitation and contracts.]** ~~This includes both major applications and general~~

~~support systems as defined by OMB Circular A-130. Examples of tasks that require security provisions include—~~

~~(1) Hosting of DOT e-Government sites or other IT operations;~~

~~(2) Acquisition, transmission, or analysis of data owned by DOT with significant replacement cost should the contractor's copy be corrupted; and~~

~~(3) Access to DOT general support systems/major applications at a level beyond that granted the general public, *e.g.,* bypassing a firewall.~~

(b) The Contractor shall develop, provide, implement, and maintain an IT Security Plan [in accordance with the statement of work and ~~. This plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of IT resources developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall~~ comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002 **[and Federal and DOT policies and procedures set forth in the statement of work, performance work statement or other requirements document]**. ~~The plan shall meet IT security requirements in accordance with Federal and DOT policies and procedures, as amended during the term of this contract, which include, but are not limited to the following:~~

~~(1) OMB Circular A-130, Managing Information as a Strategic Resource;~~

~~(2) National Institute of Standards and Technology (NIST) Guidelines;~~

~~(3) DOT CIO IT Policy (CIOP) compendium and associated guidelines;~~

~~(4) DOT Order 1630.2C, Personnel Security Management; and~~

~~(5) DOT Order 1351.37, Departmental Cyber Security Policy.~~

~~(c) Within 30 days after contract award, the contractor shall submit the IT Security Plan to the DOT Contracting Officer for review. This plan shall detail the approach contained in the offeror's proposal or sealed bid. Upon acceptance by the Contracting Officer, the Plan shall be incorporated into the contract by contract modification.~~

~~(d) Within six (6) months after contract award, the Contractor shall submit written proof of IT Security accreditation to the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with DOT policy available from the Contracting Officer upon request. The Contractor shall submit along with this accreditation a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. The accreditation and accompanying documents, to include a final security plan, risk assessment, security test and evaluation, and disaster~~

~~recovery/continuity of operations plan, upon acceptance by the Contracting Officer, will be incorporated into the contract by contract modification.~~

~~(e) On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the IT Security Plan remains valid.~~

~~(f) The Contractor shall ensure that the official DOT banners are displayed on all DOT systems (both public and private) operated by the Contractor that contain Privacy Act information before allowing anyone access to the system. The DOT CIO will make official DOT banners available to the Contractor.~~

~~(g)~~ **[(c)]** The Contractor ~~shall~~ **[must]** screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for DOT or interconnected to a DOT network in accordance with DOT Order 1630.2C**[,]** Personnel Security Management, as amended. **[The Contractor shall immediately notify the Contracting Officer when an employee who has access to DOT information systems or data terminates employment.]**

~~(h)~~ **[(d)]** ~~The Contractor shall ensure that its~~ **[All]** employees performing services under this contract **[must take]** ~~receive~~ annual IT security training in accordance with **[requirements outlined in the statement of work, and sign Rules of Behavior.]**~~OMB Circular A-130, FISMA, and NIST requirements, as amended, with a specific emphasis on rules of behavior.~~

~~(i)~~ **[(e)]** The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases and personnel used in performance of the contract. The Contractor shall provide access to enable a program of IT inspection (to include vulnerability testing), investigation, and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of DOT data or to the function of information technology systems operated on behalf of DOT), and to preserve evidence of computer crime.

~~(j)~~ **[(f)]** The Contractor shall ~~incorporate and flow down~~ **[insert]** the substance of this clause[, **including this paragraph (f), in]** ~~to~~ all subcontracts that meet the conditions in paragraph (a) of this clause.

~~(k) The Contractor shall immediately notify the Contracting Officer when an employee who has access to DOT information systems or data terminates employment.~~

(End of clause)

1252.239-71 ~~Information Technology Security Plan and Accreditation.~~ [RESERVED] [(DEC 2026)(RFO DEVIATION)]

~~As prescribed in 1239.106-70, insert the following provision:~~

~~Information Technology Security Plan and Accreditation (NOV 2022)~~

~~All offers submitted in response to this solicitation shall address the approach for completing the security plan and accreditation requirements in clause 1252.239-70, Security Requirements for Unclassified and Sensitive Information Technology Resources.~~

~~(End of provision)~~

1252.239-72 ~~Compliance with Safeguarding DOT Sensitive Data Controls.~~ [RESERVED] [(DEC 2026)(RFO DEVIATION)]

~~As prescribed in TAR 1239.7003(a), insert the following clause:~~

~~Compliance With Safeguarding DOT Senitive Data Controls (NOV 2022)~~

~~(a) The Contractor shall implement security requirements contained in clause 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting, for all DOT sensitive data on all Contractor information systems that support the performance of this contract.~~

~~(b) Contractor information systems not part of an information technology service or system operated on behalf of the Government as part of this contract are not subject to the provisions of this clause.~~

~~(c) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" at *https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final* that are in effect at the time the solicitation is issued or as authorized by the contracting officer.~~

~~(d) 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 —~~

~~(1) Why a particular security requirement is not applicable; or~~

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

~~(e) 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 Contracting Officer will incorporate accepted variance(s) from NIST SP 800-171, Rev. 2 into any resulting contract.~~

~~(End of clause)~~

1252.239-73 ~~Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.~~ [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

~~Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information (NOV 2022)~~

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

~~*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.~~

~~*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.~~

~~*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.~~

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

~~*DOT 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.~~

~~(b) *Restrictions.* (1) The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract derived from a third-party's reporting of~~

~~a cyber incident, pursuant to TAR clause, 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting (or derived from such information obtained under that clause):~~

~~(2) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting, and shall not be used for any other purpose.~~

~~(3) The Contractor shall protect the information against unauthorized release or disclosure.~~

~~(4) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.~~

~~(5) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.~~

~~(6) A breach of these obligations or restrictions may subject the Contractor to—~~

~~(i) Criminal, civil, administrative, and contractual penalties and other appropriate remedies; and~~

~~(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third-party beneficiary of this clause.~~

~~(c) *Subcontract flowdown requirement.* The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered DOT sensitive data and cyber incident reporting, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties.~~

~~(End of clause)~~

1252.239-74 Safeguarding DOT Sensitive Data and Cyber Incident Reporting. [(DEC 2026)(RFO DEVIATION)]

As prescribed in 1239.~~7003(c)~~**[171(b)]**, insert the following clause:

Safeguarding DOT Sensitive Data and Cyber Incident Reporting ~~(NOV 2022)~~ [(DEC 2026)] [(RFO DEVIATION)]

~~(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 **[must]** 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)~~ **[(a)]** *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). **[The cyber incident report shall be treated as information created by or for DOT.]**

~~(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)~~ **[(b)]** *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~~**[a]**) 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)~~ **[(c)]** *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~~**[a]**) 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)~~ **[(d)]** *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)~~ **[(e)]** *Subcontract***[***s***]** ~~*flowdown requirements*~~. The Contractor shall **[insert the substance of this clause, including this paragraph (e), 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.] [Subcontractors are required to 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 (a) of this clause.] —**

~~(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)

1252.239-75 DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements. [(DEC 2026)(RFO DEVIATION)]

As prescribed in 1239.~~7104~~**[171(c)]**, insert the following clause:

DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements ~~(NOV 2022)~~ [(DEC 2026)] [(RFO DEVIATION)]

(a) *Compliance with standards.* To the extent **[the]** Contractor creates, maintains, acquires, discloses, uses, or has access to **[personally identifiable information] [(]**PII**[)]** in furtherance of the contract, **[the]** Contractor shall comply with all applicable Federal law, guidance, and standards and DOT policies pertaining to its protection. Contractor shall notify DOT in writing immediately upon the discovery that Contractor is no longer in compliance with DOT data protection standards with respect to any PII.

(b) *Unanticipated threats.* 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.

(c) *Privacy Act.* The Contractor ~~will~~**[must]**—

(1) Comply with the Privacy Act of 1974, 5 U.S.C. 552a, DOT implementing regulations (49 CFR part 10), and DOT policies issued under the Act in the design, development, and/or operation of any system of records on individuals to accomplish a DOT function when the contract specifically identifies the work that the Contractor is to perform.

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, and/or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (c), in all subcontracts awarded under this contract which requires the design, development, and/or operation of such a system of records.

(d) *Privacy Act records.* The Contractor shall not release records subject to the Privacy Act except by the direction of the DOT, regardless of whether DOT or the Contractor maintains the records.

(e) *Confidentiality agreement.* Contractor agrees to execute a confidentiality agreement protecting PII, when necessary, and further agrees not to appropriate such PII for its own use or to disclose such information to third parties unless specifically authorized by DOT in writing.

(f) *Surrender of records.* If at any time during the term of the Contract any part of PII, in any form, that Contractor obtains from or on behalf of DOT ceases to be required by Contractor for the performance of its obligations under the Contract, or upon termination of the Contract, whichever occurs first, Contractor shall, within ten (10) business days, notify DOT and securely return such PII to DOT, or, at DOT's written request destroy, un-install and/or remove all copies of such PII in Contractor's possession or control, or such part of the PII which relates to the part of the Contract which is terminated, or the part no longer required, as appropriate, and certify to DOT that the requested action has been completed.

(g) *NIST FIPS 140-2.* At a minimum, the Contractor shall protect all PII created, collected, used, maintained, or disseminated on behalf of the Department using controls consistent with Federal

Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards, unless otherwise authorized by the DOT Chief Privacy Officer.

(h) *Protection of sensitive information.* The Contractor ~~shall~~ **[must]** comply with Government and DOT guidance for protecting PII.

(i) *Breach.* The Contractor ~~shall~~ bear**[s]** all costs, losses, and damages resulting from the Contractor's breach of these clauses. Contractor agrees to release, defend, indemnify, and hold harmless DOT for claims, losses, penalties, and damages and costs to the extent arising out of Contractor's, or its subcontractor's, negligence, unauthorized use or disclosure of PII and/or Contractor's, or its subcontractor's, breach of its obligations under these clauses.

~~(j)~~ **[(1)]** *Breach reporting.* Contractors shall report breaches involving PII directly to DOT at (202) 385-4357 or 1-(866)-466-5221 within two (2) hours of discovery. Contractor shall provide the incident number automatically assigned by DOT for all breaches reported by the Contractor or any subcontractors to the Contracting Officer.

~~(k)~~ **[(2)]** *Applicability.* Contractor ~~shall~~ **[must]** inform all principals, officers, employees, agents and subcontractors engaged in the performance of this contract of the obligations contained in these clauses.

~~(l)~~ **[(j)]** *Training.* To the extent necessary and/or required by law, the Contractor ~~shall~~ **[must]** provide training to employees, agents, and subcontractors to promote compliance with these clauses. The Contractor is liable for any breach of these clauses by any of its principals, officers, employees, agents, and subcontractors.

~~(m)~~ **[(k)]** *Subcontractor engagement.* When the Contractor engages a subcontractor in connection with its performance under the contract, and the Contractor provides such subcontractor access to PII, the Contractor ~~shall~~ **[must]** provide the Contracting Officer with prompt notice of the identity of the subcontractor and the extent of the role that the subcontractor will play in connection with the performance of the contract. This obligation is in addition to any limitations of subcontracting and consent to subcontract requirements identified elsewhere in the clauses and provisions of this contract.

~~(n)~~ **[(l)]** *Subcontract**[s]*** ~~*flowdown requirements*~~*.* Contractors shall ~~flow down~~ **insert the substance of]** this clause[**, including this paragraph (l),]** to all subcontracts and purchase orders or other agreements and require that subcontractors **[flow down]** ~~incorporate~~ this clause in their subcontracts~~, appropriately modified for identification of the parties~~. The Contractor shall enforce the terms of the clause, including action against its subcontractors, their employees and associates, or third-parties, for noncompliance. All subcontractors given access to any PII must agree to—

(1) Abide by the ~~clauses~~ **[terms]** set forth herein, including, without limitation, provisions relating to compliance with data privacy standards for the Protection of Data about Individuals, Breach Notification Controls, and Notice of Security and/or Privacy Incident;

(2) Restrict use of PII only for subcontractor's internal business purposes and only as necessary to render services to Contractor in connection with Contractor's performance of its obligations under the contract;

(3) ~~Certify~~**[Confirm]** in writing, upon completion of services provided by a subcontractor, that the subcontractor has returned to the Contractor all records containing PII within 30 days of subcontractor's completion of services to Contractor. Failure of subcontractor to return all records containing PII within this period will be reported to DOT as a privacy incident; and

(4) **[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 (a) of this clause.]**

~~(4) Report breaches involving PII directly to DOT at (202) 385-4357 or 1-(866)-466-5221 within two (2) hours of discovery. Subcontractors shall provide the incident report number automatically assigned by DOT to the prime contractor. Lower-tier subcontractors, likewise, shall report the incident report number automatically assigned by DOT to their higher-tier subcontractor until the prime contractor is reached. Contractor shall provide the DOT incident number to the Contracting Officer.~~

(End of clause)

1252.239-76 ~~Cloud Computing Services.~~ [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

~~Cloud Computing Services (NOV 2022)~~

~~(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* paragraphs (b)(5) and (d) 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 (b)(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. [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Data Jurisdiction (NOV 2022)

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)

1252.239-78 Validated Cryptography for Secure Communications. [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Validated Cryptography for Secure Communications (NOV 2022)

(a) The Contractor shall use only cryptographic mechanisms that comply with ____ [*Contracting Officer insert FIPS 140-2 level #*]. All deliverables shall be labeled ____ [*Contracting Officer insert appropriate label such as "For Official Use Only" (FOUO) or other DOT-agency selected designation per document sensitivity*].

(b) External transmission/dissemination of ____ [*Contracting Officer fill in: e.g., labeled deliverables*] to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with ____ [*Contracting Officer shall insert the standard, such as FIPS PUB 140-2, "Security requirements for Cryptographic Modules."*

(End of clause)

1252.239-79 Authentication, Data Integrity, and Non-Repudiation. [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Authentication, Data Integrity, and Non-Repudiation (NOV 2022)

The Contractor shall provide a [*Fill in: Contracting Officer fill in the "cloud service" name*] system that implements ____ [*Contracting Officer insert the required level (1-4) of FIPS 140-2 encryption standard*] that provides for origin authentication, data integrity, and signer non-repudiation.

(End of clause)

1252.239-80 Audit Record Retention for Cloud Service Providers. [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Audit Record Retention for Cloud Service Providers (NOV 2022)

(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 email archiving applications to store email, 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)

1252.239-81 Cloud Identification and Authentication (Organizational Users) Multi-Factor Authentication. [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Cloud Identification and Authentication (Organizational Users) Multi-Factor Authentication (NOV 2022)

The Contractor shall support a secure, multi-factor method of remote authentication and authorization to identified Government Administrators that will allow Government-designated personnel the ability to perform management duties on the system. The Contractor shall support multi-factor authentication in accordance with 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, and OMB implementation guidance for personal identity verification.

(End of clause)

1252.239-82 Identification and Authentication (Non-Organizational Users). [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Identification and Authentication (Non-Organizational Users) (NOV 2022)

The Contractor shall support a secure, multi-factor method of remote authentication and authorization to identified Contractor Administrators that will allow Contractor designated personnel the ability to perform management duties on the system as required by the contract.

(End of clause)

1252.239-83 **Incident Reporting Timeframes. [RESERVED] [(DEC 2026)(RFO DEVIATION)]**

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

Incident Reporting Timeframes (NOV 2022)

(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)

1252.239-84 Media Transport. [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Media Transport (NOV 2022)

(a) The Contractor shall document activities associated with the transport of DOT information stored on digital and non-digital media and employ cryptographic mechanisms to protect the confidentiality and integrity of this information during transport outside of controlled areas. This applies to—

(1) Digital media containing DOT or other Federal agency or other sensitive or third-party provided information that requires protection must be encrypted using FIPS 140-2 [*Contracting Officer insert required encryption mode, based on FIPS 199 risk category*] when transported outside of controlled areas; and

(2) Nondigital media must be secured using the same policies and procedures as paper.

(b) Contractors shall ensure accountability for media containing DOT or other Federal agency or other sensitive or third-party provided information that is transported outside of controlled areas. This can be accomplished through appropriate actions such as logging and a documented chain of custody form.

(c) DOT or other Federal agency sensitive or third-party provided information that resides on mobile/portable devices (*e.g.*, USB flash drives, external hard drives, and SD cards) must be encrypted using FIPS 140-2 [*Contracting Officer insert the required encryption mode based on FIPS 199 risk category*]. All Federal agency data residing on laptop computing devices must be protected with NIST-approved encryption software.

(End of clause)

1252.239-85 Personnel Screening—Background Investigations. [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Personnel Screening—Background Investigations (NOV 2022)

(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)

1252.239-86 Boundary Protection—Trusted Internet Connections. [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

Boundary Protection—Trusted Internet Connections (NOV 2022)

The Contractor shall ensure that Federal information, other than non-sensitive information, being transmitted from Federal government entities to external entities using cloud services is inspected by Trusted internet Connections (TIC) processes or the Contractor shall route all external connections through a Trusted internet Connection (TIC).

~~(End of clause)~~

1252.239-87 ~~Protection of Information at Rest.~~ [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

~~Protection of Information at Rest and in Transit (NOV 2022)~~

~~The Contractor shall provide security mechanisms for handling data at rest and in transit in accordance with FIPS 140-2 ___ [*Contracting officer insert encryption standard, based on NIST FIPS 199 categorization*].~~

~~(End of clause)~~

1252.239-88 ~~Security Alerts, Advisories, and Directives.~~ [RESERVED] [(DEC 2026)(RFO DEVIATION)]

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

~~Security Alerts, Advisories, and Directives (NOV 2022)~~

~~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)~~

1252.239-89 Technology Modernization [and Upgrades/Refreshment]. [(DEC 2026)(RFO DEVIATION)]

As prescribed in 1239.~~7303(a)~~**[7001]**, insert the following clause:

Technology Modernization [and Upgrades/Refreshment] (~~NOV 2022~~[DEC 2026]) [(RFO DEVIATION)]

(a) [*Postaward.* After the issuance of the contract, the Government may solicit, and the Contractor is encouraged to propose independently, either a modernization or an upgrade/refreshment approach to the original equipment offered under the contract.]

[(1)] *Modernization approach.* ~~After issuance of the contract, the Government may solicit, and the Contractor is encouraged to propose independently, a modernization approach to the hardware, software, specifications, or other requirements of the contract.~~ This modernization approach may be proposed to increase efficiencies (both system and process level), reduce costs, or strengthen the cyber security posture, or for any other purpose which presents an advantage to

the Government. Furthermore, the modernization approach should, to the maximum extent practicable, align with how the commercial sector would solve the problem.

[(2) *Upgrade/refreshment approach.* These improvements may be proposed to save money, to improve performance, to save energy, to satisfy increased data processing requirements, or for any other purpose that presents a technological advantage to the Government. As part of the proposed changes, the Contractor shall submit a price or cost proposal to the Contracting Officer for evaluation. Those proposed technology improvements that are acceptable to the Government will be processed as modifications to the contract.]

(b) *Proposal requirements.* As part of the proposed changes, the Contractor shall submit a price or cost proposal to the Contracting Officer for evaluation. Those proposed modernized improvements that are acceptable to the Government will be processed as modifications to the contract. At a minimum, the Contractor shall submit the following information with each proposal:

(1) A summary of how the modernized proposal aligns with the commercial sector approach and how the current approach is out of alignment/differs;

(2) A description of the difference between the existing contract requirement and the proposed change, and the comparative advantages and disadvantages of each;

(3) Itemized requirements of the contract that must be changed if the proposal is adopted and the proposed revision to the contract for each such change;

(4) An estimate of the changes in performance and price or cost, if any, that will result from adoption of the proposal;

(5) An evaluation of the effects the proposed changes would have on collateral costs to the Government, such as Government-furnished property costs, costs of related items, and costs of maintenance, operation and conversion (including Government application software);

(6) A statement of the schedule for contract modification adopting the proposal that maximizes benefits of the changes during the remainder of the contract, including supporting rationale; and

(7) Identification of impacts on contract cost and schedule. The Government is not liable for proposal preparation costs or for any delay in acting upon any proposal submitted pursuant to this clause.

(c) *Withdrawal.* The Contractor has a right to withdraw, in whole or in part, any proposal not adopted by contract modification within the period specified in the proposal. The decision of the Contracting Officer whether to accept any such proposal under this contract is final and not subject to the "Disputes" clause of this contract.

(d) *Product testing.* If the Government wishes to test and evaluate any item(s) proposed, the Contracting Officer will issue written directions to the Contractor specifying what item(s) will be

tested, where and when the item(s) will be tested, to whom the item(s) is to be delivered, and the number of days (not to exceed 90 calendar days) that the item will be tested.

(e) *Contract modification.* The Contracting Officer may accept any proposal submitted pursuant to this clause by giving the Contractor written notice thereof. This written notice will be given by issuance of a modification to the contract. Until the Government issues a modification incorporating a proposal under this contract, the Contractor shall remain obligated to perform in accordance with the requirements, terms, and conditions of the existing contract.

(f) *Change orders.* If a proposal submitted pursuant to this clause is accepted and applied to this contract, the equitable adjustment increasing or decreasing the price or cost-plus-fixed-fee (CPFF) shall be in accordance with the procedures of the applicable "Changes" clause incorporated by reference in the contract. The resulting contract modification will state that it is made pursuant to this clause.

(End of clause)

1252.239-90 ~~Technology Upgrades/Refreshment.~~ [RESERVED] [(DEC 2026)(RFO DEVIATION)]

~~As prescribed in 1239.7303(b), insert the following clause:~~

~~Technology Upgrades/Refreshment (NOV 2022)~~

~~(a) *Upgrade/refreshment approach.* After issuance of the contract, the Government may solicit, and the Contractor is encouraged to propose independently, technology improvements to the hardware, software, specifications, or other requirements of the contract. These improvements may be proposed to save money, to improve performance, to save energy, to satisfy increased data processing requirements, or for any other purpose that presents a technological advantage to the Government. As part of the proposed changes, the Contractor shall submit a price or cost proposal to the Contracting Officer for evaluation. Those proposed technology improvements that are acceptable to the Government will be processed as modifications to the contract. As a minimum, the following information shall be submitted by the Contractor with each proposal:~~

~~(1) A description of the difference between the existing contract requirement and the proposed change, and the comparative advantages and disadvantages of each;~~

~~(2) Itemized requirements of the contract that must be changed if the proposal is adopted, and the proposed revision to the contract for each such change;~~

~~(3) An estimate of the changes in performance and price or cost, if any, that will result from adoption of the proposal;~~

~~(4) An evaluation of the effects the proposed changes would have on collateral costs to the Government, such as Government-furnished property costs, costs of related items, and costs of maintenance, operation and conversion (including Government application software);~~

~~(5) A statement of the time by which the contract modification adopting the proposal must be issued so as to obtain the maximum benefits of the changes during the remainder of the contract including supporting rationale; and~~

~~(6) Identification of any impacts to contract completion time or delivery schedule. The Government is not liable for proposal preparation costs or for any delay in acting upon any proposal submitted pursuant to this clause. The Contractor has a right to withdraw, in whole or in part, any proposal not adopted by contract modification within the period specified in the proposal. The decision of the Contracting Officer whether to accept any such proposal under this contract is final and not subject to the "Disputes" clause of this contract.~~

~~(b) *Test and evaluation.* If the Government wishes to test and evaluate any item(s) proposed, the Contracting Officer will issue written directions to the Contractor specifying what item(s) will be tested, where and when the item(s) will be tested, to whom the item(s) is to be delivered, and the number of days (not to exceed 90 calendar days) that the item will be tested. The Contracting Officer may accept any proposal submitted pursuant to this clause by giving the Contractor written notice thereof. This written notice will be given by issuance of a modification to the contract. Unless and until a modification is executed to incorporate a proposal under this contract, the Contractor shall remain obligated to perform in accordance with the requirements, terms and conditions of the existing contract. If a proposal submitted pursuant to this clause is accepted and applied to this contract, the equitable adjustment increasing or decreasing the price or CPFF shall be in accordance with the procedures of the applicable "Changes" clause incorporated by reference in Section I of the contract. The resulting contract modification will state that it is made pursuant to this clause.~~

~~(End of clause)~~

1252.239-91 Records Management. [(DEC 2026)(RFO DEVIATION)]

As prescribed in 1239.~~7403~~**[7103]**, insert the following clause:

Records Management (~~NOV 2022~~[DEC 2026)] [(RFO DEVIATION)]

(a) *Definition.*

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.

(b) *Requirements.* (1) *Compliance.* Contractor 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. Such Federal records ~~shall~~**[must]** be managed and scheduled for disposition only as permitted by the Federal Records Act, other relevant statutes or regulations, and DOT Order 1351.28, Departmental Records Management Policy.

(3) *Records maintenance.* While DOT records are in the Contractor's custody, the Contractor is responsible for preventing the alienation or unauthorized destruction of 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, Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records, for reporting to NARA.

(4) *Unauthorized disclosure.* The Contractor ~~shall~~**[must]** notify the Contracting Officer within two hours of discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor ~~shall~~**[must]** ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment. The Contractor ~~shall~~**[may]** 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. When information, data, documentary material, records and/or equipment is no longer required, ~~it shall be returned to DOT control or~~ the Contractor must **[return it to DOT control or]** hold it until otherwise directed. Items returned to the Government ~~shall~~**[may]** 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 in accordance with the contract.

(c) *Non-public information.* The Contractor shall not create or maintain any records containing any non-public DOT information that are not specifically authorized by the contract.

(d) *Rights in data.* ~~Rights in data under this contract are set forth in clauses prescribed by FAR part 27 and included in this contract, (*e.g.,* 52.227-14 Rights in Data – General).~~ The Contractor must make any assertion of copyright in the data or other deliverables under this contract and substantiate such assertions **[(see 52.227-14, Rights in Data – General)].** The Contractor must add or correct all limited rights, restricted rights, or copyright notices and take all other appropriate actions in accordance with the terms of this contract and the clauses included herein.

(e) *Notification of third-party access requests.* The Contractor ~~shall~~**[must]** notify the Contracting Officer promptly of any requests from a third party for access to Federal records, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency. The Contractor shall cooperate with the Contracting Officer to take all measures to protect Federal records~~,~~ from any unauthorized disclosure.

(f) *Training.* All Contractor employees ~~assigned to~~ **[under]** this contract who create, work with, or otherwise handle records are required to take DOT-provided records management training. The Contractor is responsible for confirming to the Contracting Officer that training, including initial training and any annual or refresher training, has been completed in accordance with agency policies.

(g) *Subcontract***[s]** ~~*flowdown requirements.*~~ ~~(1)~~ The Contractor shall ~~incorporate~~ **[insert]** the substance of this clause, **[including this paragraph (g),]** ~~its terms and requirements including this paragraph (g),~~ in all subcontracts ~~under this contract, and require written subcontractor acknowledgment of same~~.

~~(2) Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.~~

(End of clause)

1252.239-92 ~~Information and Communication Technology Accessibility Notice.~~
[RESERVED] [(DEC 2026)(RFO DEVIATION)]

~~As prescribed in 1239.203-70(a), insert the following provision:~~

~~**Information and Communication Technology Accessibility Notice (NOV 2022)**~~

~~(a) Any offeror responding to this solicitation must comply with established DOT Information and Communication Technology (ICT) (formerly known as Electronic and Information (EIT)) accessibility standards. Information about Section 508 is available at *https://www.section508.gov/*.~~

~~(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 1252.239-93, Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies and services meet applicable Section 508 accessibility standards, offerors must submit appropriate Section 508 Checklists, in accordance with the checklist completion instructions. The purpose of the checklists is to assist DOT acquisition and program officials in determining whether proposed ICT supplies or information, documentation and services support conform to applicable Section 508 accessibility standards. The checklists allow offerors or developers to self-evaluate their supplies and document—in detail—whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues.~~

~~(c) Respondents to this solicitation must identify any exception to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, *i.e.*, after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.~~

~~(End of provision)~~

1252.239-93 Information and Communication Technology Accessibility. [(DEC 2026)(RFO DEVIATION)]

As prescribed in 1239.~~203-70(b)~~**[171(d)]**, insert the following clause:

Information and Communication Technology Accessibility (~~NOV 2022~~[DEC 2026]) (RFO DEVIATION)

(a) All Information and Communication Technology (ICT) supplies, information, documentation and services support developed, acquired, maintained or delivered under this contract or order must comply with the Information and Communication Technology (ICT) Standards and Guidelines (*see* 36 CFR parts 1193 and 1194). Information about Section 508 is available at *https://www.section508.gov/*.

(b) The Section 508 accessibility standards applicable to this contract or order are identified in the Specification, Statement of Work, or Performance Work Statement. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

~~(c) The Section 508 accessibility standards applicable to this contract are: ___ [*Contracting Officer inserts the applicable Section 508 accessibility standards*].~~

(d) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer

may require that the Contractor submit a completed Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If the Government determines that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) If this is an indefinite-delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies or services will define the specifications and accessibility standards for the order **[and the requirements in paragraph (d) apply]**. ~~In those cases, the Contractor may be required to provide a completed Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.~~

(End of clause)

[1252.239-94 Use of Government Furnished Equipment or Information —Official, Unofficial, and Personal International Travel. [(DEC 2026)(RFO DEVIATION)]

As prescribed in 1239.272, insert the following clause:

Use of Government Furnished Equipment or Information —Official, Unofficial, and Personal International Travel (DEC 2026) (RFO DEVIATION)

Unless the contracting officer provides authorization for DOT official international travel and DOT standard issued Government Furnished Equipment (GFE) is provided, the contractor is prohibited from using GFE or personal equipment to conduct Department of Transportation (DOT) business or access DOT data and information systems outside of the United States or its territories. This prohibition applies, but is not limited to, while on personal, unofficial, or official travel.

(End of clause)]