TRANSPORTATION ACQUSITION MANUAL (TAM)

NOTE NO. 2026-02

Effective Date: 1 December 2026

SUMMARY OF ITEMS

TAM PART 1239

TAM Note 2026-02 is issued under the authority of the RFO TAR 1201.103, Authority, and 1201.201, Policy, and TAM 1201.301-70. This TAM Note incorporates interim language removed from TAR Part 1239 and now to be placed, via this TAM Note, into TAM Part 1239 for placement into a statement of work (SOW), performance work statement, or other requirements document(s) for all applicable solicitations and contracts involving acquiring information and communications technology (ICT) and supplies and services that use ICT, as prescribed below.

Background

On April 15, 2025, Executive Order (E.O.) 14275, Restoring Common Sense to Federal Procurement was signed. 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. As a part of the RFO initiative, the OSPE has issued a series of RFO Transportation Acquisition Regulation (TAR) class deviations (CDs) to the Transportation Acquisition Regulation (TAR) to streamline the TAR and align with the RFO FAR parts. Text determined to be non-regulatory, but necessary, is being reviewed, revised when applicable, and placed in DOT's internal guidance such as the Transportation Acquisition Manual (TAM) or other agency guidance controlled by offices other than the Office of the Senior Procurement Executive (e.g., the Office of the Chief Digital and Information Officer (OCDIO) in the case of RFO TAR Part 1239 CD and TAM Part 1239).

To ensure alignment with issued E.O.s and the associated RFO FAR part CD, it is necessary for DOT to issue the RFO TAR CD for TAR Part 1239 in advance of a proposed rule to implement these requirements to ensure DOT policies and procedures align with the FAR and TAR. Based on the substantive content in the existing TAR Part 1239 and ongoing review and update of DOT ICT and other

related policy and guidance, applicable “removed” text from the TAR is still applicable to DOT acquisitions but is now placed in TAM Part 1239 on an interim basis.

Impacts to TAM Part 1239

As a result of revisions to TAR Part 1239 issued as a part of the RFO TAR Part 1239 class deviation, certain removed text (including certain solicitation provisions and contract clauses) from the TAR is being placed in the **TAM, Appendix A**, until such time as the Office of the Chief Digital and Information Officer (OCDIO) publishes internal guidance that replaces this TAM material. This part prescribes newly **numbered requirements terms and conditions (T&Cs)** (former TAR Part 1239 provisions and clauses) to insert in solicitations and contracts via the statement of work (SOW), performance work statement (PWS), or other requirements documents in accordance with TAM Part 1239, Appendix A guidance.

As OCDIO completes their complete ICT and related policy reviews, some Appendix A and other TAM Part 1239 guidance will likely be revised and reissued separately via an OCDIO Information Technology Implementation Memorandum (ITIM), and later via other OCDIO policy issuances.

These former TAR "solicitation provisions and contract clauses" now placed in TAM Part 1239, Appendix A, are now be referred to as **"requirements terms and conditions (T&Cs)"** and must be placed in solicitation and contract statements of work (SOW's), performance work statements (PWS's), and other requirements document(s) as prescribed in the TAM Part 1239 and Appendix A.

This material has been renumbered from a TAR clause or provision to the T&C numbers as shown. The titles have remained the same for ease of transition.

Note: DOT intends on conducting further analysis and developing a rule for publication in the Federal Register for public comment after the release of the RFO TAR CD, the TAM Note for TAM Part 1239 (including Appendix A), and a later issued OCDIO ITIM on any updated IT, ICT, and ICT-related internal agency guidance. This will be analyzed as a part of the 1DOT consolidation, ongoing OCDIO policy review and updates, and as related FAR proposed and final rules are published.

ACTION:

Insert the following Appendix A numbered requirements terms and conditions (T&C) in applicable solicitation or contract statements of work (SOWs), performance work statements (PWS's), and other requirements document(s) as prescribed in these TAM instructions.

- The terms and conditions in **TAM Part 1239, Appendix A**, are currently prescribed in TAR part 1239, Code of Federal Regulations (CFR).

- As a part of the Revolutionary FAR Overhaul (RFO) analysis performed on the TAR, this text is ***removed*** from the TAR and ***placed*** temporarily in the TAM via the RFO TAR Part 1239 class deviation.

Contracting Officers, along with Program Managers/Project Managers and Contracting Officer's Representatives, for applicable acquisitions set forth in the Appendix A prescriptions must—

1. Jointly examine as an acquisition team TAM Part 1239 and Appendix A Requirement T&Cs;
2. Determine which applicable prescribed numbered requirements terms and conditions in Appendix A (e.g., T&C 1239.01, T&C 1239.05, etc.) apply for applicable ICT and related acquisitions in conjunction with a review of TAR Part 1239, TAM Part 1239, and Appendix A to TAM Part 1239; *and*
3. Place the numbered requirement T&Cs (see Appendix A) in solicitation and contract statements of work (SOWs), performance work statements (PWS's) and other requirements document(s), when applicable and in accordance with the prescriptions contained in the Appendix or the TAM.
4. Obtain signed coordination and concurrence from the cognizant OCDIO representative and requiring activity that Appendix A requirement terms and condition have been reviewed and those that will be included in solicitation and contract SOWs, PWS's, and other requirements documents have been included.
5. File this documentation in the electronic contract file prior to solicitation release and contract award.

PART 1239—ACQUISITION OF INFORMATION [AND COMMUNICATION] TECHNOLOGY

[1239.001 Applicability.
1239.001-70 Definitions.
1239.001-71 Policy.
1239.001-72 Identification of Information Technology and the IT acquisition process.

SUBPART 1239.1--PRESOLICITATION
1239.101-70 Scope of subpart.
1239.101-71 Definitions.
1239.170 Policy.
1239.104 ICT accessibility standards.
1239.104-1 Scope.
1239.104-270 Procedures.

SUBPART 1239.70—TECHNOLOGY MODERNIZATION, UPGRADES AND REFRESHMENT
1239.7000 Scope of subpart.
1239.7002 Policy.

SUBPART 1239.71 [RESERVED]

SUBPART 1239.72—INFORMATION SECURITY AND INCIDENT RESPONSE REPORTING
1239.7200 Scope of subpart.
1239.7201 Definitions.
1239.7202 Policy.

SUBPART 1239.73—PROTECTION OF DATA ABOUT INDIVIDUALS
1239.7300 Scope of subpart.
1239.7301 Definitions.
1239.7302 Policy.
1239.7303 Responsibilities.

SUBPART 1239.74—CLOUD COMPUTING
1239.7400 Scope of subpart.
1239.7401 Definitions.
1239.7402 Policy.
1239.7403 DOT FedRAMP specific requirements.

SUBPART 1239.75—REQUIREMENTS TERMS AND CONDITIONS
1239.7500 Scope of subpart.
1239.7501 Prescriptions for requirements terms and conditions.

APPENDIX A: Requirements Terms and Conditions

TAM Part 1239 – APPENDIX A – Requirements Terms and Conditions (T&Cs)

T&C 1239.01 Security Requirements for Unclassified Information Technology Resources. (DEC 2026)
T&C 1239.02 Information Technology Security Plan and Accreditation. (DEC 2026)
T&C 1239.03 Compliance with Safeguarding DOT Sensitive Data Controls. (DEC 2026)
T&C 1239.04 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. (DEC 2026)
T&C 1239.05 Safeguarding DOT Sensitive Data and Cyber Incident Reporting. (DEC 2026)
T&C 1239.06 DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements. (DEC 2026)
T&C 1239.07 Cloud Computing Services. (DEC 2026)
T&C 1239.08 Data Jurisdiction. (DEC 2026)
T&C 1239.09 Validated Cryptography for Secure Communications. (DEC 2026)
T&C 1239.10 Authentication, Data Integrity, and Non-Repudiation. (DEC 2026)
T&C 1239.11 Audit Record Retention for Cloud Service Providers. (DEC 2026)
T&C 1239.12 Cloud Identification and Authentication (Organizational Users) Multi-Factor Authentication. (DEC 2026)
T&C 1239.13 Identification and Authentication (Non-Organizational Users). (DEC 2026)
T&C 1239.14 Incident Reporting Timeframes. (DEC 2026)
T&C 1239.15 Media Transport. (DEC 2026)
T&C 1239.16 Personnel Screening—Background Investigations. (DEC 2026)
T&C 1239.17 Boundary Protection—Trusted Internet Connections. (DEC 2026)
T&C 1239.18 Protection of Information at Rest. (DEC 2026)
T&C 1239.19 Security Alerts, Advisories, and Directives. (DEC 2026)
T&C 1239.20 Information and Communication Technology Accessibility Notice. (DEC 2026)
T&C 1239.21 Information and Communication Technology Accessibility. (DEC 2026)]

SUBPART 1239.1--GENERAL 2
1239.101 Policy. 2
1239.170 Identification of Information Technology and the IT Acquisition Process 5

SUBPART 1239.1--GENERAL

1239.101 Policy.

(g) (1) All procurement requests regardless of dollar value – including requests for purchase card transactions – containing Information Technology (IT), as defined in FAR 2.101 and TAM 1202.101, must have the request approved by the DOT Chief Information Officer (CIO) (or designee) before it can be processed. The DOT CIO (or designee) approval must be obtained by including the procurement action in the Operating Administration (OA) IT Spend Plan process and receiving an IT Procurement Approval Memorandum indicating the procurement action was approved. Further clarification of how to identify IT and the procurement actions needed to receive an approved IT Procurement Approval Memorandum can be found here in Frequently Asked Questions (FAQ). Details on how to leverage the IT Spend Plan process to receive an IT Procurement Approval Memorandum can be found below in subsection (h) and TAM 1239.170. For further guidance on IT Spend Plan approval, please contact your designated Capital Planning and Investment Control (CPIC) coordinator listed here or email the CPIC mailbox at CPIC@dot.gov.

(2) All IT procurements at DOT must abide by DOT's OCIO policies and operational guidance, which can be found at https://usdot.sharepoint.com/sites/CIOITPolicy.

(3) An approved IT Procurement Approval Memorandum serves as the DOT CIO approval for all DOT acquisition plans.

(i)Interim Approval. OAs may submit interim procurement request (IPR) approvals to the DOT CIO (or designee) when a time sensitive purchase/procurement must be processed and has not been approved via the quarterly IT Spend Plan review process. To request an IPR, OAs shall submit the request to ITSpendApproval@dot.gov. If approved, the DOT CIO (or designee) will provide an email confirmation, which shall serve as the interim IT Procurement Approval Memorandum until such time the OA can formally submit the request via the quarterly IT Spend Plan process.

(4) The table below outlines IT procurement actions and the requirement of the DOT CIO's (or designee) approval before the procurement action can be solicited or awarded by the contracting officer.

Category	Action	Approved IT Spend Plan Needed?
New Procurement	Purchase at or below the Micro-Purchase Threshold	YES
New Procurement	Purchase Order above the Micro-Purchase Threshold up to the Simplified Acquisition Threshold (SAT)	YES
New Procurement	Contract above the SAT	YES
New Procurement	Blanket Purchase Agreement (BPA)	YES
New Procurement	Task/Delivery Order (TO/DO), BPA Call	YES
New Procurement	Inter-/Intra-agency Agreement (IAA) subject to FAR 17.5 and TAM 1217.5	YES
New Procurement	Basic Ordering Agreement	YES
Modification	Option Year/Period Exercise on all award types (including IAAs subject to FAR 17.5 and TAM 1217.5	YES
Modification	Funding Only	NO
Modification	Change Order (i.e., supplemental agreement for additional work, negotiated changes, etc.)	YES
Modification	Termination (any type)	NO
Modification	Closeout	NO
Contract Mod.	No Cost Administrative Mod	NO

(5) Procurement Strategy Changes Necessitating Re-Approval by the DOT CIO (or designee). When the DOT CIO (or designee) approves a procurement action in the IT Spend Plan process, that approval is based on the information provided at that time. If details change on a procurement action between the time of DOT CIO approval via the IT Spend Plan (i.e. issuance of the IT Procurement Approval Memorandum) and the time of procurement request acceptance by the contracting office (or any time thereafter prior to award), then the procurement action may require re-approval by the DOT CIO (or designee). The table below shows the changes made to a procurement action after it has been approved in the IT Spend Plan process and the necessity for re-approval by the DOT CIO (or designee). If a procurement action requires re-approval, then the procurement information in the IT Spend Plan must be updated and the IT Spend Plan must be re-submitted to the DOT CIO (or designee) for review at ITSpendApproval@dot.gov. If the procurement action receives re-approval, then a new IT Procurement Approval Memorandum shall be included in the requirements package.

IT Procurement Information	Change Since Approval from the DOT CIO (via the IT Spend Plan)	Procurement Action Needs to be Re-Approved by the DOT CIO

Scope of Work	Change in the scope of work or requirements.	YES
Approved Procurement Vehicle	Proposed procurement vehicle is changed	YES
Period of Performance (POP)	Length of period of performance changes by more than 6 months	YES
Total Procurement Value	Total procurement value changes +/- 20%	YES
Candidate to Transition to DOT Enterprise Contract?	Answer is changed from 'yes' to 'no'	YES
All Other Information	Any change	NO

(6) Steps to Follow if a contracting officer determines that a procurement contains IT, but no evidence of OCIO approval is attached. The contracting officer shall send a documented email back to the Requisitioner stating that there is no evidence of OCIO approval and to provide the required documentation so the purchase request (PR) package can be processed. The contracting officer **shall not** proceed with the solicitation or award until evidence of approval via the IT Procurement Approval Memo is received.

i. If the Requisitioner does not comply with the requirements of this subsection (i.e. Needing approval via the IT Spend Plan), please send an email to ITSpendApproval@dot.gov and reference the following:

A) PR Number, Requisitioner' s Name and PR amount
B) OA and POC for OCIO follow-up

ii. If a Requisitioner requires IT Spend Plan approval assistance, the contracting officer shall refer them to their designated OA CPIC coordinator to guide them through the process. OA CPIC coordinators can be found here.

(h) Exceptions. Procurements processed by the John A. Volpe National Transportation Systems Center (Volpe Center) for the Federal Aviation Administration (FAA) or non-DOT customers are not required to comply with the DOT IT Spend Plan requirements as outlined in this Chapter.

(i) Chief Information Officer (CIO) and IT Acquisition Process

The following figure provides an overview of the process to coordinate and involve the OCIO in the IT acquisition planning process. If a procurement action contains IT, then the workflow shown directly below shall be followed.

~~1239.170 Identification of Information Technology and the IT Acquisition Process~~

~~Information Technology costs are frequently embedded or coupled within many of the contracts throughout the department. To ensure that these procurements are correctly identified as having IT-related spend within them, refer to Frequently Asked Questions (FAQ) found here for additional guidance. This will help Acquisition Planners determine if the procurement contains IT, and if it does, then the procurement will need to be included in the OA IT Spend Plan submission for DOT CIO review and approval. If the procurement action is approved, then an IT Procurement Approval Memorandum will be provided by the DOT CIO to show evidence of approval.~~

[PART 1239 - ACQUISITION OF INFORMATION AND COMMUNICATION TECHNOLOGY

1239.001 Applicability.

(a)(1) This part prescribes policies and procedures for the following—

(i) Acquiring information and communications technology (ICT), supplies and services that use ICT, including Federal and other policy requirements;

(ii) Section 508 standards and compliance for contracts;

(iii) Information security and incident response reporting;

(iv) Protection of data about individuals;

(v) Technology modernization and upgrade/refreshment; and

(vi) Record management.

1239.001-70 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.**

1239.001-71 Policy.

(a) All procurement requests regardless of dollar value – including requests for purchase card transactions – containing information technology (IT), as defined in FAR 2.101 and TAM 1202.101, must have the request approved by the DOT Chief Digital and Information Officer (OCDIO) (or designee) before it can be processed. The DOT CDIO (or designee) approval must be obtained by including the procurement action in the Operating Administration (OA) IT

Spend Plan process and receiving an IT Procurement Approval Memorandum indicating the procurement action was approved.

(1) Further clarification of how to identify IT and the procurement actions needed to receive an approved IT Procurement Approval Memorandum can be found here in Frequently Asked Questions (FAQ). Details on how to leverage the IT Spend Plan process to receive an IT Procurement Approval Memorandum can be found below and at TAM 1239.170. For further guidance on IT Spend Plan approval, please contact your designated Capital Planning and Investment Control (CPIC) coordinator listed here or email the CPIC mailbox at CPIC@dot.gov.

(2) All IT procurements at DOT must abide by DOT's OCDIO policies and operational guidance, which can be found at https://usdot.sharepoint.com/sites/CIOITPolicy.

(b) An approved IT Procurement Approval Memorandum serves as the DOT CDIO approval for all DOT acquisition plans.

(1) Interim Approval. OAs may submit interim procurement request (IPR) approvals to the DOT CDIO (or designee) when a time sensitive purchase/procurement must be processed and has not been approved via the quarterly IT Spend Plan review process. To request an IPR, OAs must submit the request to ITSpendApproval@dot.gov. If approved, the DOT CDIO (or designee) will provide an email confirmation, which will serve as the interim IT Procurement Approval Memorandum until such time the OA can formally submit the request via the quarterly IT Spend Plan process.

(2) The table below outlines IT procurement actions and the requirement of the DOT CIO's (or designee) approval before the procurement action can be solicited or awarded by the contracting officer.

Table 1 to 1239.001-71, IT Procurement Actions and DOT OCDIO Approval Requirements

Category	Action	Approved IT Spend Plan Needed?
New Procurement	Purchase at or below the Micro-Purchase Threshold	YES
New Procurement	Purchase Order above the Micro-Purchase Threshold up to the Simplified Acquisition Threshold (SAT)	YES
New Procurement	Contract above the SAT	YES

New Procurement	**Blanket Purchase Agreement (BPA)**	**YES**
New Procurement	**Task/Delivery Order (TO/DO), BPA Call**	**YES**
New Procurement	**Inter-/Intra-agency Agreement (IAA) subject to FAR subpart 17.5, Interagency Acquisitions, and TAM subpart 1217.5**	**YES**
New Procurement	**Basic Ordering Agreement**	**YES**
Modification	**Option Year/Period Exercise on all award types (including IAAs subject to FAR subpart 17.5 and TAM subpart 1217.5) Note: See FAR 17.204-1, Exercise of Options, and FAR Companion Guide (FC) FC 17.204-1.**	**YES**
Modification	**Funding Only**	**NO**
Modification	**Change Order (i.e., supplemental agreement for additional work, negotiated changes, etc.)**	**YES**
Modification	**Termination (any type)**	**NO**
Modification	**Closeout**	**NO**
Contract Mod.	**No Cost Administrative Mod**	**NO**
New Procurement	**Purchase Order above the Micro-Purchase Threshold up to the Simplified Acquisition Threshold (SAT)**	**YES**

(c) Procurement Strategy Changes Necessitating Re-Approval by the DOT CDIO (or designee). When the DOT CDIO (or designee) approves a procurement action in the IT Spend Plan process, that approval is based on the information provided at that time. If details change on a procurement action between the time of DOT CDIO approval via the IT Spend Plan (i.e., issuance of the IT Procurement Approval Memorandum) and the time of procurement request acceptance by the contracting office (or any time thereafter prior to award), then the procurement action may require re-approval by the DOT CDIO (or designee). The table below shows the changes made to a procurement action after it has been approved in the IT Spend Plan process and the necessity for re-approval by the DOT CDIO (or designee). If a procurement action requires re-approval, then the procurement information in the IT Spend Plan must be updated and the IT Spend Plan must be re-submitted to the DOT CDIO (or designee) for review at ITSpendApproval@dot.gov. If the procurement action receives re-approval, then a new IT Procurement Approval Memorandum shall be included in the requirements package.

IT Procurement Information	Change Since Approval from the DOT CDIO (via the IT Spend Plan)	Procurement Action Needs to be Re-Approved by the DOT CDIO
Scope of Work	**Change in the scope of work or requirements.**	**YES**
Approved Procurement Vehicle	**Proposed procurement vehicle is changed**	**YES**
Period of Performance (POP)	**Length of period of performance changes by more than 6 months**	**YES**

Total Procurement Value	**Total procurement value changes +/- 20%**	**YES**
Candidate to Transition to DOT Enterprise Contract?	**Answer is changed from 'Yes' to 'No'**	**YES**
All Other Information	**Any change**	**NO**

(d) Steps to Follow if a contracting officer determines that a procurement contains IT, but no evidence of OCDIO approval is attached. The contracting officer shall send a documented email back to the Requisitioner stating that there is no evidence of OCDIO (or designee) approval and to provide the required documentation so the purchase request (PR) package can be processed. The contracting officer shall not proceed with the solicitation or award until evidence of approval via the IT Procurement Approval Memo is received.

(1) If the Requisitioner does not comply with the requirements of this subsection (i.e. Needing approval via the IT Spend Plan), please send an email to ITSpendApproval@dot.gov and reference the following:

(i) PR Number, Requisitioner' s Name and PR amount.
(ii) OA and POC for OCDIO follow-up.

(2) If a Requisitioner requires IT Spend Plan approval assistance, the contracting officer shall refer them to their designated OA CPIC coordinator to guide them through the process. OA CPIC coordinators can be found here.

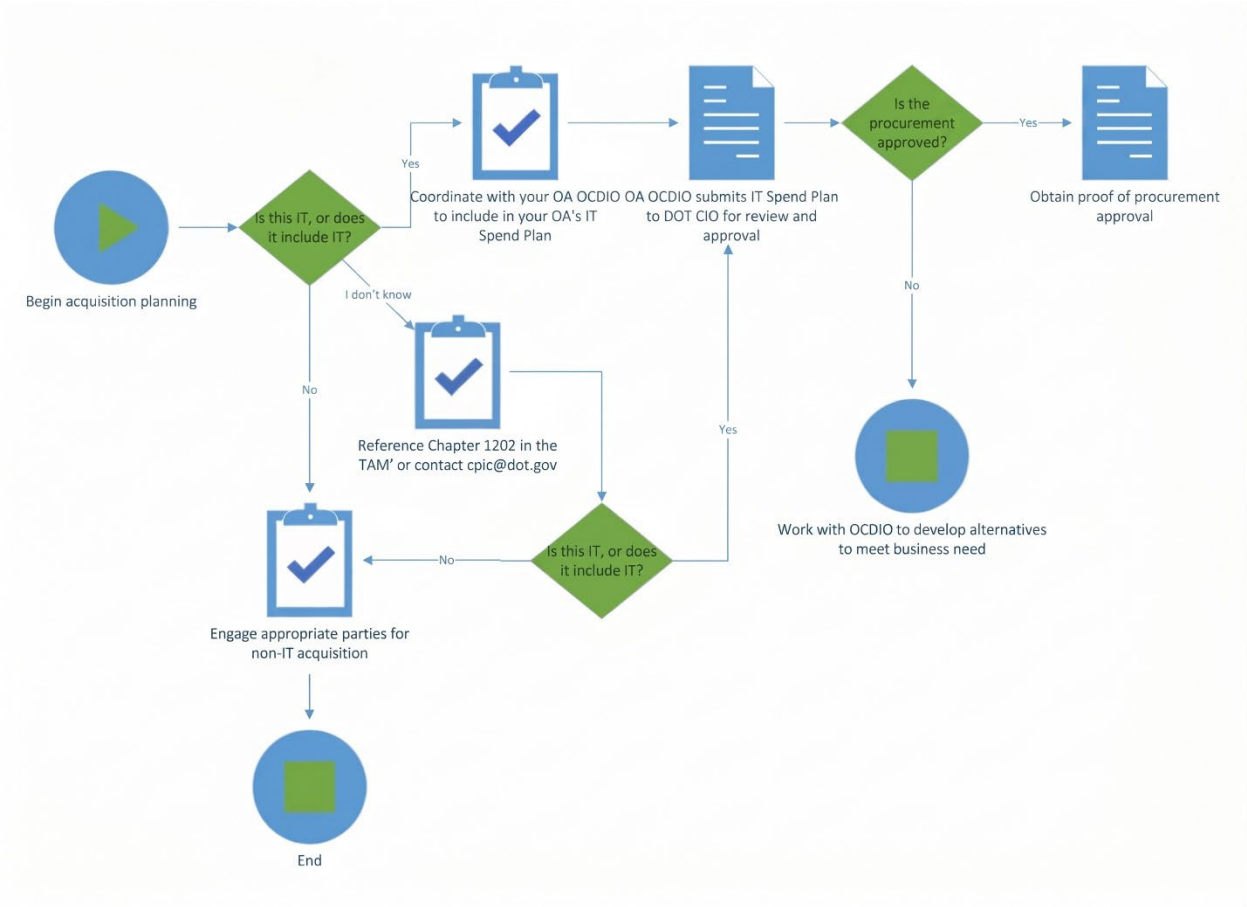
(3) Exceptions. Procurements processed by the John A. Volpe National Transportation Systems Center (Volpe Center) for the Federal Aviation Administration (FAA) or non-DOT customers are not required to comply with the DOT IT Spend Plan requirements as outlined in this part.

1239.001-72 Identification of Information Technology and the IT acquisition process.

(a) Information Technology costs are frequently embedded or coupled within many of the contracts throughout the department. To ensure that these procurements are correctly identified as having IT-related spend within them, refer to Frequently Asked Questions (FAQ) found here for additional guidance. This will help Acquisition Planners determine if the procurement contains IT, and if it does, then the procurement will need to be included in the OA IT Spend Plan submission for DOT CDIO review and approval. If the procurement action is approved, then an IT Procurement Approval Memorandum will be provided by the DOT CDIO to show evidence of approval.

(b) Chief Digital and Information Officer (CDIO) and IT Acquisition Process. The following figure provides an overview of the process to coordinate and involve the ODCIO in the IT acquisition planning process. If a procurement action contains IT, then the workflow shown directly below shall be followed. See Figure 1 to 1239.001-72.

Figure 1 to 1239.001-72.



SPACE DELIBERATELY LEFT BLANK

Subpart 1239.1—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.**

1239.170 Policy.

The acquisition of products or services supporting the development or maintenance of DOT information and communication technology (ICT) and services (see TAR 1239.170) and DOT software applications, systems, and infrastructure, must contain appropriate requirements established by the Federal Acquisition Regulation (FAR), other Federal statutes, OMB Guidance, other Federal policies and guidance, and DOT policy. This includes Requirements Terms and Conditions (T&Cs) required by this Note and Appendix A (DEC 2026), Information and Communications Technology (ICT); and Information, Information Systems, and Related Services – Requirements Terms and Conditions (T&Cs). Place requirements T&Cs in applicable solicitations and contracts statements of work, performance work statements, and other requirements documents as set forth in the prescriptions in this part at 1239.7501.

1239.104 ICT accessibility standards.

1239.104-1 Scope.

This section implements DOT policy on section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and ICT accessibility standards (see FAR 39.104).

1239.104-270 Procedures.

(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*.

(b) See the prescription for requirements T&C 1239.20 and T&C 1239.21 at 1239.7501(t) and (u).

Subpart 1239.70—Technology Modernization and Upgrades/Refreshment

1239.7000 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.

1239.7002 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 and requirements terms and conditions as may be required by the Federal Acquisition Regulation (FAR), TAR, and other Federal authorities, in order to ensure that information system modernization is prioritized accordance with Federal law, OMB Guidance, and DOT policy. During Postaward orientation, cover the requirements of the TAR clause prescribed at TAR 1239.7001.

Subpart 1239.71 [RESERVED]

Subpart 1239.72—Information Security and Incident Response Reporting

1239.7200 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.

1239.7201 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.**

1239.7202 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. 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.

Subpart 1239.73—Protection of Data About Individuals

1239.7300 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 TAR subpart 1224.1) and privacy in the acquisition of information technology in this subpart and Appendix A. DOT rules and regulations implementing the Privacy Act of 1974 are located at 49 CFR part 10.

1239.7301 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.**

1239.7302 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.

1239.7303 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 TC 1239.06, 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 will ensure contractors are aware of and will implement the clause prescribed at TAR 1239.372, TAR clause 1252.239-94, 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.

Subpart 1239.74—Cloud Computing

1239.7400 Scope of subpart.

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

1239.7401 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.**

1239.7402 Policy.

(a) ***General.*** **Generally, DOT entities must 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 will 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 must 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 Digital Information Officer (CDIO), 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 CDIO; 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 CDIO.

(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.

1239.7403 DOT FedRAMP specific requirements.

DOT entities will set forth DOT FedRAMP specific cloud service requirements. DOT cloud service providers must 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 and the TAR, 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 T&C 1239.09 prescribed at 1239.7501(i).**

(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 and requiring activities (e.g., Program/Project Managers and Contracting Officer Representative's (CORs) must specify what level (1-4) of FIPS 140-2 encryption is required. See T&C 1239.10 prescribed at 1239.7501(j).

(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 T&C 1239.11 prescribed at 1239.7501(k).**

(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 T&C 1239.12 prescribed at 1239.7501(l).**

(e) ***Identification and authentication (non-organizational users).*** **Contracting officers must require that Cloud Service Providers pursuing a FedRAMP authorization provide multi-factor authentication for the provider's administrators. See T&C 1239.13 prescribed at 1239.7501(m).**

(f) ***Incident reporting timeframes.*** **Contracting officers must 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 must include specific incident reporting requirements including who and how to notify the agency. See T&C 1239.14 prescribed at 1239.7501(n).**

(g) ***Media transport.*** **DOT or other Federal agency information and data require protection. Contracting officers and program offices must set forth specific DOT media transport requirements. See T&C 1239.15 prescribed at 1239.7501(o).**

(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 TAR clause 1252.204-70 and T&C 1239.16 prescribed at 1239.7501(p).**

(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, contract clauses and SOW T&Cs. These**

support personnel shall undergo required DOT background investigations prior to providing services and performing on the contract. See TAR clause 1252.204-70, paragraph (b) and T&C 1239.16 prescribed at 1239.7501(p). 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.

SUBPART 1239.75—REQUIREMENTS TERMS AND CONDITIONS

1239.7500 Scope of subpart.

1239.7501 Prescriptions for requirements terms and conditions.

Insert requirements terms and conditions (T&Cs) in solicitation and contract statements of work (SOWs), performance work statements (PWSs), and other requirements documents as follows:

(a) Insert T&C 1239.01, Security Requirements for Unclassified Information Technology Resources, in all solicitations and contracts exceeding the micro-purchase threshold that include ICT.

(b) Insert T&C 1239.02, Information Technology Security Plan and Accreditation, in all solicitations and contracts exceeding the micro-purchase threshold that include ICT information technology services.

(c) Insert T&C 1239.03, 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.

(d) Insert T&C 1239.04, 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.

(e) Insert T&C 1239.05, 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.

(f) Insert T&C 1239.06, 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.

(g) Insert T&C 1239.07, 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.

(h) Insert T&C 1239.08, 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.

(i) Insert T&C 1239.09, 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.

(j) Insert T&C 1239.10, 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.

(k) Insert T&C 1239.11, 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.

(l) Insert T&C 1239.12, 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.

(m) Insert T&C 1239.13, 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.

(n) Insert T&C 1239.14, 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.

(o) Insert T&C 1239.15, 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.

(p) Insert T&C 1239.16, 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.

(q) Insert T&C 1239.17, 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.

(r) Insert T&C 1239.18, 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.

(s) Insert T&C 1239.19, 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.

(t) Insert T&C 1239.20, Information and Communication Technology Accessibility Notice, in all solicitations.

(u) Insert T&C 1239.21, Information and Communication Technology Accessibility, in all solicitations.

APPENDIX A

Information and Communications Technology (ICT); and Information, Information Systems, and Related Services

Required Terms and Conditions (T&C)

For

Applicable Solicitations and Contracts

Insert Appendix A: Requirements Terms and Conditions in solicitations and contracts for information and communications technology (ICT) acquisitions including acquisitions involving information, information systems, and information technology-related services and supplies in accordance with the prescriptions in Appendix A for each numbered terms and conditions (T&C).

T&C 1239.01 Security Requirements for Unclassified Information Technology Resources. (DEC 2026)

As prescribed in 1239.7501(a), insert the following T&C:

Security Requirements for Unclassified Information Technology Resources (DEC 2026)

(a) In addition to the requirements in TAR clause 1252.239-70, Security Requirements for Unclassified Information Technology Resources (DEC 2026)(RFO DEVIATION), information technology and information systems that fall under the stated requirements include 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-developed IT Security Plan must 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 must describe those parts of the contract to which these terms and conditions. Follow the requirements of the contract clause, this T&C, and other Federal and DOT policies and procedures set forth in the statement of work, performance work statement or other requirements documents. 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 must submit the IT Security Plan to the DOT Contracting Officer for review. This plan must detail the approach contained in the offeror's proposal or sealed bid. Upon acceptance by the Contracting Officer, the Plan will be incorporated into the contract by contract modification.

(d) Within six (6) months after contract award, the Contractor must 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 must 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 must 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 CDIO will make official DOT banners available to the Contractor.

(g) As stated in the contract clause, the Contractor 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) All employees performing services under this contract must take annual IT security training in accordance with requirements outlined in the statement of work or performance work statement, and sign Rules of Behavior, and OMB Circular A-130, FISMA, and NIST requirements, as amended, with specific emphasis on rules of behavior.

(i) In accordance with TAR clause 1252.239-70, Security Requirements for Unclassified Information Technology Resources (DEC 2026)(RFO DEVIATION), 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) The Contractor must immediately notify the Contracting Officer when an employee who has access to DOT information systems or data terminates employment.

(End of T&C)

T&C 1239.02 Information Technology Security Plan and Accreditation. (DEC 2026)

As prescribed in 1239.7501(b), insert the following T&C:

Information Technology Security Plan and Accreditation (DEC 2026)

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 (DEC 2026)(RFO DEVIATION).

(End of T&C)

T&C 1239.03 Compliance with Safeguarding DOT Sensitive Data Controls. (DEC 2026)

As prescribed in 1239.7501(c), insert the following T&C:

Compliance With Safeguarding DOT Sensitive Data Controls (DEC 2026)

(a) The Contractor shall implement security requirements contained in clause 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting (DEC 2026) (RFO DEVIATION), 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 T&C.

(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 Digital and Information Officer (CDIO), 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 DOT Office of the CDIO 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 T&C)

T&C 1239.04 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. (DEC 2026)

As prescribed in 1239.7501(d), insert the following T&C:

Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information (DEC 2026)

(a) *Definitions.* As used in this T&C—

***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 (DEC 2026)(RFO DEVIATION) (or derived from such information obtained under that clause and this T&C).**

(2) The Contractor must 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 (DEC 2026)(RFO DEVIATION) and this T&C, and such information 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 T&C and clause 122.239-74 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 T&C.

(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 T&C.

(c) ***Subcontracts.*** **The Contractor shall include these terms and conditions (T&C), 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 T&C)

T&C 1239.05 Safeguarding DOT Sensitive Data and Cyber Incident Reporting. (DEC 2026)

As prescribed in 1239.7501(e), insert the following T&C:

Safeguarding DOT Sensitive Data and Cyber Incident Reporting (DEC 2026

(a) *Definitions.* As used in this T&C—

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 this T&C or clause 1252.239-74 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 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 T&C 1239.07, 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 T&C, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(iv) of this T&C, 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 T&C 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 T&C, 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 TAR clause 1252.239-70, Security Requirements for Unclassified Information Technology Resources (DEC 2026)(RFO DEVIATION).

(c) *Cyber incident reporting requirement.* See TAR clause 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting (DEC 2026)(RFO DEVIATION. Comply with the requirements stated therein including—

(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 T&C 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 in accordance with TAR clause 1252.239-74, paragraph (b), the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with the clause and this T&C.**

(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 T&C or TAR clause 1252.239-74, that includes Contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor must 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 T&C 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 T&C 1239.04, 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) *Compliance with laws and regulations on electronic communications*. The Contractor is required to conduct activities under this T&C and TAR clauses 1252.239-74 and 1252.239-75, and in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(m) *Subcontracts*. Comply with this T&C and TAR clause 1252.239-74 and 1253.239-75 and subcontract flowdown requirements. Contractors must ensure to include this T&C and the required TAR clauses 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 T&C or referenced TAR 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 T&C; 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 T&C.

(End of T&C)

T&C 1239.06 DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements. (DEC 2026)

As prescribed in 1239.7501(f), insert the following T&C:

DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements (DEC 2026)

Contractors shall report breaches involving PII directly to DOT at (202) 385-4357 or 1-(866)-466-5221 within two (2) hours of discovery. Subcontractors must provide the incident report number

automatically assigned by DOT to the prime contractor. Lower-tier subcontractors, likewise, must report the incident report number automatically assigned by DOT to their higher-tier subcontractor until the prime contractor is reached. The Contractor must provide the DOT incident number to the Contracting Officer.

(End of T&C)

T&C 1239.07 Cloud Computing Services. (DEC 2026)

As prescribed in 1239.7501(g), insert the following T&C:

Cloud Computing Services (DEC 2026)

(a) *Definitions.* As used in this T&C—

***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 T&C 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 T&C) 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 T&C.**

(j) ***Subcontracts.*** **The Contractor shall include this T&C, including this paragraph (j), in all subcontracts that involve or may involve cloud services, including subcontracts for commercial products or commercial services.**

(End of T&C)

T&C 1239.08 Data Jurisdiction. (DEC 2026)

As prescribed in 1239.7501(h), insert the following T&C:

Data Jurisdiction (DEC 2026)

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 T&C)

T&C 1239.09 Validated Cryptography for Secure Communications. (DEC 2026)

As prescribed in 1239.7501(i), insert the following T&C:

Validated Cryptography for Secure Communications (DEC 2026)

(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 T&C)

T&C 1239.10 Authentication, Data Integrity, and Non-Repudiation. (DEC 2026)

As prescribed in 1239.7501(j), insert the following T&C:

Authentication, Data Integrity, and Non-Repudiation (DEC 2026)

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 T&C)

T&C 1239.11 Audit Record Retention for Cloud Service Providers. (DEC 2026)

As prescribed in 1239.7501(k), insert the following T&C:

Audit Record Retention for Cloud Service Providers (DEC 2026)

(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 T&C)

T&C 1239.12 Cloud Identification and Authentication (Organizational Users) Multi-Factor Authentication. (DEC 2026)

As prescribed in 1239.7501(l), insert the following T&C:

Cloud Identification and Authentication (Organizational Users) Multi-Factor Authentication (DEC 2026)

The Contractor shall support a secure, multi-factor method of remote authentication and authorization to identify 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 T&C)

T&C 1239.13 Identification and Authentication (Non-Organizational Users). (DEC 2026)

As prescribed in 1239.7501(m), insert the following T&C:

Identification and Authentication (Non-Organizational Users) (DEC 2026)

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 T&C)

T&C 1239.14 Incident Reporting Timeframes. (DEC 2026)

As prescribed in 1239.7501(n), insert the following T&C:

Incident Reporting Timeframes (DEC 2026)

(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 T&C)

T&C 1239.15 Media Transport. (DEC 2026)

As prescribed in 1239.7501(o), insert the following T&C:

Media Transport (DEC 2026)

(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 T&C)

T&C 1239.16 Personnel Screening—Background Investigations. (DEC 2026)

As prescribed in 1239.7501(p), insert the following T&C:

Personnel Screening—Background Investigations (DEC 2026)

(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 T&C)

T&C 1239.17 Boundary Protection—Trusted Internet Connections. (DEC 2026)

As prescribed in 1239.7501(q), insert the following T&C:

Boundary Protection—Trusted Internet Connections (DEC 2026)

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 T&C)

T&C 1239.18 Protection of Information at Rest. (DEC 2026)

As prescribed in 1239.7501(r), insert the following T&C:

Protection of Information at Rest and in Transit (DEC 2026)

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 T&C)

T&C 1239.19 Security Alerts, Advisories, and Directives. (DEC 2026)

As prescribed in 1239.7501(s), insert the following T&C:

Security Alerts, Advisories, and Directives (DEC 2026)

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 T&C)

T&C 1239.20 Information and Communication Technology Accessibility Notice. (DEC 2026)

As prescribed in 1239.7501(t), insert the following T&C:

Information and Communication Technology Accessibility Notice (DEC 2026)

(a) The Section 508 accessibility standards applicable to this solicitation are stated in TAR clause 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.

(b) 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 T&C)

T&C 1239.21 Information and Communication Technology Accessibility. (DEC 2026)

As prescribed in 1239.7501(u), insert the following T&C:

Information and Communication Technology Accessibility (DEC 2026)

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

(b) Postaward -- task or delivery orders. 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 T&C)]

Any questions relating to the above changes may be directed to DOTAcquisitionPolicy@dot.gov.

CHRISHAUN PATRICE JONES

Digitally signed by CHRISHAUN PATRICE JONES
Date: 2026.11.02 14:55:15 -05'00'

Chrishaun Jones
Senior Procurement Executive
Office of the Senior Procurement Executive
United States Department of Transportation