

## TAR Final Rule 2105-AE26

### Summary of Differences Contained in Information Collections

#### No Public Comments Received

This is submitted to close open OMB statement from DOT's request for approval of information collection requirements for the following Information Collection Requests (ICR) Reference Numbers for the OMB review that concluded interim review:

- 202202-2105-001
- 202202-2105-002
- 202202-2105-003
- 202201-2105-002
- 202201-2105-003

Final approval is requested for the five assigned PRA OMB Control Numbers: 2105-0578, 2105-0579, 2105-0580, 2105-0581, and 2105-0582

The following five groups of PRA ICs are included under the proposed TAR NPRM and the TAR Final Rule. OMB Assigned these provisional OMB Control Numbers pending official approval (as of 5/31/22):

- 2105-0578 - Part 1239 Clauses: 1252.239-76, 1252.239-77, 1252.239-80, 1252.239-83, 1252.239-85, and 1252.239-88
  - 2105-0579 - Part 1239 Clause: 1252.239-75
  - 2105-0580 - Part 1239 Clauses: 1252.239-89 and 1252.239-90
  - 2105-0581 - Part 1239 Clause: 1252.239-70
  - 2105-0582 - Part 1239 Clauses: 1252.239-72 and 1252.239-74
- o **PRA Group 1:**
    - 1252.239-70, Security Requirements for Unclassified Information Technology Resources.
  - o **PRA Group 2:**
    - 1252.239-72, Compliance with Safeguarding DOT Sensitive Data Controls.
    - 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting.
  - o **PRA Group 3:**
    - 1252.239-75, DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements.
  - o **PRA Group 4:**
    - 1252.239-76, Cloud Computing Services.
    - 1252.239-77, Data Jurisdiction.
    - 1252.239-80, Audit Record Retention for Cloud Service Providers.
    - 1252.239-83, Incident Reporting Timeframes.

- 1252.239-85, Personnel Screening—Background Investigations.
- 1252.239-88, Security Alerts, Advisories, and Directives.
- o **PRA Group 5:**
  - 1252.239-89, Technology Modernization.
  - 1252.239-90, Technology Upgrades/Refreshment.

## Background

DOT published a proposed rule in the Federal Register at 86 FR 69452 on December 7, 2021, to amend the TAR to implement and/or supplement the FAR. Please refer to the proposed rule for a discussion of the reasons why DOT proposed the changes to the TAR described in that rule document.

DOT provided a 60-day comment period for the public to respond to the proposed rule and submit comments. The public comment period closed on February 7, 2022. DOT received no public comments on the proposed rule and no public comments were received on any of the information collection requirements in the rule. The final rule includes provisions constituting new collections of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3521) that require approval by the Office of Management and Budget (OMB). Accordingly, under 44 U.S.C. 3507(d), DOT submitted the information collections to OMB for review and approval. No comments were received on the proposed collections of information. If OMB does not approve the collections of information as requested, DOT will immediately remove the provisions containing a collection of information or take such other action as directed by OMB.

The only revisions to the proposed clauses (information collection requirements) now contained in the final rule pertain to technical non-substantive revisions to comport with new Federal Acquisition Regulation terminology, correction of grammar, references, etc., as described below.

This rule adopts as a final rule the proposed rule published in the Federal Register on December 7, 2021, except for technical non-substantive changes to update terminology in accordance with FAR final rules and other minor administrative amendments as shown in the paragraphs that follow. This rule establishes a 2022 baseline edition of the TAR.

#### Technical Non-Substantive Changes to the Rule

This rule makes the non-substantive changes to the proposed rule described in the following paragraphs to provide clarity, eliminate confusion, and ensure compliance with the Federal Acquisition Regulation (FAR). Specifically, DOT is revising the term “commercial items” to reflect either “commercial products and commercial services” or “commercial products or commercial services” in alignment with FAR final rule, **Federal Acquisition Regulation: Revision of Definition of “Commercial Item”**, RIN 9000-AN76, effective December 6, 2021. There are 28 mentions of the legacy term “commercial items” that were identified in the TAR proposed rule amendatory language in various TAR parts, subparts, and sections, to include titles as well as the underlying text. The legacy term “commercial items” was also referenced in two FAR clause references where the FAR title has also been revised because of the referenced FAR final rule.

Accordingly, DOT is revising the TAR final rule to reflect the updated terminology in accordance with the FAR final rules as reflected in the amendatory text as follows:

1. Under section 1252.239-74, Safeguarding DOT Sensitive Data, and Cyber Incident Reporting, in paragraph (o), *Subcontract flowdown requirement*, subparagraph (1) of the clause, DOT is revising the phrase “commercial items” to read, “commercial products or commercial services.”

2. Under section 1252.239-76, Cloud Computing Services, in paragraph (j) *Subcontract flowdown requirement*, DOT is revising the phrase “commercial items” to read, “commercial products or commercial services.” Additionally, DOT is revising the TAR final rule to revise the use of the terminology from “electronic and information technology (EIT)” to the FAR updated usage of “Information and Communication Technology” as shown below in item number 14.
3. Additionally, the following minor administrative corrections were made to reflect appropriate citation references in accordance with the U.S. Government Publishing Office (GPO) Style Manual and the FAR Drafting Guide:
  - Under section 1252.239-75, DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements, paragraph (c) (1), the reference to “49 CFR Part 10” is revised to read, “49 CFR part 10.”
4. Finally, in part 1252 these technical non-substantive revisions are reflected in the following provisions or clauses published in the proposed rule. These also include the following non-substantive minor administrative corrections to correct grammar or other sentence formatting and structure, as well as to provide clarity to current DOT policies and procedures:
  - a. In section 1252.239-70, Security Requirements for Unclassified Information Technology Resources, paragraph (b), the word “and” is removed after “...in accordance with Federal and DOT policies and procedures,” and the word “,which” is added after “as amended during the terms of this contract,” and word “and” is removed before “include” so the last sentence now reads: “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:”.

- b. In section 1252.239-72, Compliance with Safeguarding DOT Sensitive Data Controls, paragraph (c), DOT added the reference to “Revision 2” to the NIST 800-171 reference and title, and updated a new direct link to the cited publication at nist.gov. We also added in the Revision 2 (Rev. 2) reference in the clause at paragraphs (d), and (e).
- c. In section 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting, we revised the wording in paragraph (a) under the definition for “*Adequate security*” to remove “balance and” before the phrase “are commensurate”, and to remove “impact and” before “consequences”, to add the words “and probability” after “consequences” and to delete the word “the” before “loss, misuse,..” so the definition now reads more clearly: “*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.” In paragraphs (b)(2)(i)-(iv), references are updated, and an updated link is provided. In paragraph (b)(2)(v), the word “to” is removed before “have an alternate” so the end of the sentence now reads, “...to be nonapplicable, or have an alternative, but equally effective, security measure that may be implemented in its place.” In paragraph (b)(2)(vi) the words “the Contractor” is added after “Contracting Officer

when” to clarify who is doing the requesting and “requesting” is revised to “request”. The end of the sentence now reads as follows: “...a copy of that approval shall be provided to the Contracting Officer when the Contractor requests its recognition under this contract.” In paragraph (c)(1)(i), the word “that” is removed after “DOT sensitive data” in the second sentence, and the words “whether the incident” is added, and “affect” is revised to “affects” so the end of the last/second sentence now reads: “... in order to identify compromised DOT sensitive data or whether the incident affects the Contractor’s ability to provide operationally critical support; and...”. And in paragraph (o), *Subcontract flowdown requirements*, the reference to NIST SP 800-171 is updated to add “Rev. 2.”

- d. In section 1252.239-75, DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements, paragraph (n) *Subcontract flowdown requirements*, paragraph (n)(1), the word “its” is removed before “provisions relating to”, and the word “and” is deleted before Breach Notification...” so the sentence now reads:

“Abide by the clauses set forth herein, including, without limitation, provisions relating to compliance with data privacy standards for the Protection of Data about Individuals, Breach Notification Controls, and Notice of Security and/or Privacy Incident;”

- e. In section 1252.239-76, Cloud Computing Services, paragraph (b)(4), the reference to NIST Special Publication 800-53 is updated to reflect

“Revision 5.” In paragraph (b)(6)(ii), the phrase “DOT Order” is revised to add an “s” and to add “containing” immediately afterward so it now reads: “...FedRAMP and DOT Orders containing cybersecurity and privacy policies.” In paragraph (g), an “s” is added to “discover” and “isolate” so the beginning of the sentence now reads, “The Contractor or subcontractor(s) that discovers and isolates malicious software....”.

- f. In section 1252.239-77, Data Jurisdiction, in the first sentence the words “in which” are added after “all data centers” and the word “that” is deleted before “the data” so the beginning of the sentence now reads: “The Contractor shall identify all data centers in which the data at rest or data backup will reside,...”.
- g. In section 1252.239-85, Personnel Screening—Background Investigations, an updated active link is provided to a website containing the referenced OMB memorandum.
- h. In section 1252.239-88, Security Alerts, Advisories, and Directives, the words “who are” are added before “assigned system administration,...” and the word “who” is added after the words, “and/or security responsibilities and who are...”.
- i. In section 1252.239-89, Technology Modernization, the word “or” is added before “strengthen the cyber security posture” in the second sentence.

These minor technical nonsubstantive revisions will ensure DOT’s updated regulation is clear and contains the most recent citations, references, links, and current procedures.