## Synopsis/Solicitation: Post-Accident Toxicological Testing Oversight

### Request for Quote (RFQ) – 693JJ626Q000027 Overview- Purchase Order

The Federal Railroad Administration (FRA) intends to award a Purchase Order to provide the technical oversight services necessary for the Office of Railroad Safety, Drug and Alcohol Division to meet the requirements described in the Statement of Work (SOW). This requirement supports the FRA by providing technical and scientific oversight specializing in forensic toxicology, laboratory testing procedures, proficiency testing, and 49 CFR Part 219/Part 40 compliance review services to ensure continuing public confidence in the forensic integrity and scientific credibility of the FRA Post-Accident Toxicological Testing (PATT) Program. This is a combined synopsis/solicitation for commercial services prepared in accordance with the format in the Federal Acquisition Regulation (FAR) Overhaul, Subpart 12.201, Solicitation Procedures, as supplemented with additional information included in this notice.

The FRA will conduct this acquisition using the format in the Federal Acquisition Regulation (FAR) Overhaul (RFO) - FAR Part Deviation Guidance, Subpart 12.201, Solicitation Procedures – and anticipates awarding a PO after receipt and evaluation of qualified quotations.

The quotations will be provided to Government Officials for the purpose of assuring that the Quoter has a complete understanding of the scope of this effort and has the capability to provide a complete solution to the Statement of Work (SOW). Any quotation that is incomplete or non-compliant with any requested submission requirement of this RFQ may immediately be removed from further consideration. **Quotes that fail to include inspection team members with a Fellow (F-ABFT), Diplomate (D-ABFT-FT, D-ABFT-FA, or D-ABFT-FD), or equivalent certification from the American Board of Forensic Toxicology may be immediately removed from further consideration.**

It is the Government's intent to award a small-business set-aside purchase order to the responsible Quoter whose quotation, in conforming to the RFQ, provides the overall best-value to the Government. The total estimated value of this purchase order is estimated at $2,700,000.00.

The Government reserves the right to cancel this RFQ without award if the needs of the requirement are not met. This RFQ does not commit the Government to pay for the preparation and submission of a quotation.

The Government has assigned the North American Industry Classification System (NAICS) Code 541690 – Other Scientific and Technical Consulting Services for this procurement. The Product and Service Code (PSC) for this requirement is B529 – "Special Studies/Analysis: Scientific Data."

## 1. Introduction

### 1.1. Purpose

This Request for Quotation (RFQ) is issued to quoters to provide technical oversight, scientific review of laboratory Post-Accident Toxicological Testing (PATT) procedures, proficiency testing, compliance review services, and expert consultation to support the FRA's mission to reduce drug and alcohol abuse in the railroad industry.

### 1.2 Scope

The Technical Oversight Contractor shall provide FRA support in all technical and scientific areas which relate to the detection and deterrence of drug and alcohol use in the railroad industry pursuant to Title 49, Code of Federal Regulations, Part 219 (49 CFR Part 219) and 49 CFR Part 40. The effort focuses on ongoing technical evaluation and scientific review of the designated FRA post-accident laboratory, proficiency testing, compliance audit support, and subject matter consultation.

The Quoter must perform the required services, as defined specifically in the SOW, across the following distinct performance task areas:

**Task 1: Technical and Scientific Monitoring of Designated FRA Post-Accident Laboratory**

- **Subtask 1 - Inspection:** Conduct tri-annual comprehensive inspections of the designated FRA toxicology laboratory for compliance with FRA regulations, Department of Health and Human Services (HHS) Mandatory Guidelines, and established forensic toxicology standards College of American Pathologists (CAP), the Society of Forensic Toxicologists (SOFT), the American Board of Forensic Toxicology (ABFT), or the American Academy of Forensic Sciences (AAFS). Evaluate protocols, personnel qualifications, equipment, security, and quality assurance. Provide draft inspection reports within 30 working days and final reports within 10 working days of draft submission. Inspection team members must hold a ***Fellow of the American Board of Forensic Toxicology (F-ABFT)*****,** ***a Diplomate of the American Board of Forensic Toxicology (D-ABFT-FT, DABFT- FA, or D-ABFT-FD)*****, or** ***another equivalent credential*****,** with demonstrated experience in blood/urine screening/confirmation methodologies and post-mortem toxicology.

- **Subtask 2 - FRA Post-Accident Laboratory Proficiency Testing:** Design, implement, and operate an open proficiency testing program for the designated FRA post-accident laboratory in collaboration with the FRA SME and COR. Retain 1–2 reference laboratories to analyze blank and spiked human whole blood and urine samples covering the full range of FRA-required analytes and cutoffs. Provide findings reports within 40 working days.

**Task 2: Railroad Part 219 Compliance Review Services**

- The Quoter shall provide expert advice and/or program support services related to the detection and deterrence of drug and alcohol use in the railroad industry. Provide technical experts to assist FRA in 49 CFR Part 219 and Part 40 compliance audits of rail carriers and service providers at various national locations.

**Task 3: Expert Consultation Services**

- Provide 7-day-a-week/extended hour telephone access for expert scientific, technical, and policy advice to support the entire Part 219 and Part 40 program . Deliver immediate verbal advice followed by written advice within 24 hours. The Quoter shall be prepared to consult in

providing appropriate Part 219 and Part 40 subject matter training to the FRA inspector workforce and the railroad industry (including carrier personnel, rail labor, and program service providers) in areas requiring technical, scientific, and policy expertise including regulatory changes. Assist, as part of a joint FRA and Transport Canada (TC) working group, with joint FRA/Transport Canada working groups on cross-border operations. Support the development of program management tools (Plan-Policy builder, audit reporting tools).

**Task 4: Deliverables**

- Provide 3 Laboratory Inspection Reports per year (including QC/QA and proficiency testing analysis) and 5 Class 1 Railroad Part 219 Compliance Reviews per year electronically to the FRA SME and COR.

### 1.3 Period of Performance

The Base Period of Performance shall be one (1) year (12 months) from the effective date of award, with four (4) 12-month option periods. If all options are exercised, the total duration shall not exceed 60 months.

### 1.4 Specific Requirements

See RFQ 693JJ626Q000027 Attachment 1 – Post-Accident Toxicological Testing (PATT) Oversight Statement of Work.

### 1.5 Anticipated Contract Type

FRA anticipates awarding a Firm-Fixed-Price (FFP) Purchase Order.

## 1. Instructions

Responses to this RFQ must be submitted by the date and time listed in Table 1 of this section to the Contracting Officer (CO) by the deadline dates and times. The Contracting Officer shall provide a confirmation email if the Quotation was received.

All correspondence must have **RFQ #693JJ626Q000027** included in the subject line.

NOTE: It is the Interested Quoter's responsibility to read the RFQ and all related documents carefully. Additionally, it is the Quoter's responsibility to ensure/verify that the Government receives its submission on or before the date/time specified. **The Government reserves the right to not accept any late quotes. Please do not wait until the deadline to submit your quotation.**

**ANTICIPATED RFQ TIMELINE:** The following table provides due dates for RFQ events. These dates are subject to change.

**Table 1**

| Events | Dates | Times |
|---|---|---|
| Questions Due from Interested Quoters | August 18, 2026 | 1200 Eastern Time |
| Answers provided to Interested Quoters via RFQ Amendment | August 24, 2026 | |

| | | |
|---|---|---|
| Quotes Due | August 28, 2026 | 1200 Eastern Time |
| Award Decision | September 7, 2026 | |

Late submissions will not be evaluated unless the Contracting Officer determines that it is in the best interest of the Government.

## 2.1 Questions

If your company has questions regarding this procurement, please submit your inquiries immediately via email, no later than by the date and time listed in Table 1 to the Contracting Officer identified below:

**Name: KeriAnne Gallagher**
**Contracting Officer**
**Email: kerianne.gallagher@dot.gov**

- Questions submitted by a method other than email will not be accepted or answered.
- Any questions received after the above specified cut-off date and time will not be accepted or answered.
- All email inquiries must have "**Questions – RFQ #693JJ626Q000027**" included in the subject line.
- A Government's response shall be executed via an RFQ amendment on/about **August 24, 2026.**

## 2.2 Volumes, Page Limitations, Content, & Submission Requirements

All submissions shall be submitted electronically via email on or before the RFQ closing date as stated above. We kindly request a "no quote / no-bid reply" if your company chooses not to respond to this RFQ. A submission of a quotation shall be considered the Quoter's official quotation.

### A. Quotation Content:

| Naming Convention | Title |
|---|---|
| Volume 1 | (Cover Letter, Prior Experience Responses – Factor 1) |
| Volume 2 | (Technical & Management Approach - Factor 2) |
| Volume 3 | Price – Factor 3 |

### B. Submission Requirements

- The Quoter must have an ***active*** registration in the System for Award Management (SAM) at http://www.sam.gov.
- By submitting a quotation, the Quoter agrees to comply with all terms and conditions set forth in this Request for Quotations (RFQ).
- Quoters must email an electronic copy of each Volume to the CO no later than the specified dates and times specified in Table 1.
- DOT-FRA will not provide any technical assistance or reimburse quote submission costs.
- Submission text must use a standard, professional font (Arial or Times New Roman) at a minimum font size of 11-point. Headings may be larger (14-point or 16-point) to establish a clear visual hierarchy.

## 2.3 Required Components of Each Volume and Section

**Volume 1: Cover Letter, Prior Experience Responses – (Factor 1)**

### 2.3.1 Cover Letter

An authorized official who can obligate the Quoter shall sign a Cover Letter submitted on the Quoter's letterhead demonstrating the Quoter's intent to be bound to the purchase order terms and conditions. The cover letter shall include the following information:

1. The RFQ number.
2. UEI number.
3. Taxpayer Identification Number (TIN).
4. GSA Contract Number (if applicable)
5. Socio-Economic Status
6. The name, complete address, telephone number, and email address of the authorized official with the authority to enter into an agreement with the DOT, FRA. Provide the name and contact information for more than one representative in the event of unforeseen events.
7. If applicable, acknowledgement of all RFQ amendments issued by clearly acknowledging each amendment in the cover letter ***and*** submitting a fully executed copy of each of the Standard Form (SF) 30 Amendments.
8. The RFQ form (SF 1449, Solicitation/contract/order for commercial products and commercial services) fully executed.
9. Include a statement specifying the extent of agreement with all terms, conditions, and provisions included in the RFQ.
10. Identify any exceptions or deviations to clauses, provisions, attachments, etc. which have been incorporated into this RFQ.
11. Acknowledgement of 1252.209-70 Organizational and Consultant Conflicts of Interest (if applicable)

The cover letter shall contain no pricing information.

### 2.3.2 Factor 1: Demonstrated Prior Experience

The Quoter shall submit a summary narrative detailing at least three (3) examples of their prior experience performing contracts that demonstrate experience similar in size, scope, and/or complexity to the SOW. Examples must be projects that are ongoing or were completed within the last five (5) calendar years. Examples may include projects performed by the Quoter or the Quoter's proposed Subcontractors. However, at minimum, at least two of the examples shall be submitted for work performed by the Prime Quoter. The Government highly desires, but does not require, that each example demonstrate support of a Federal agency. Examples citing the Quoter's experience as a subcontractor may be utilized, so as long as any subcontractor experience referenced is clearly identified. However, the Government desires, but does not require, that at least one example submitted is for efforts that the Quoter performed as a prime contractor. Examples should answer the Prior Experience Questions listed below.

The summary narrative shall provide the following:

A. Customer Federal Agency
B. Program Name

C. Contract Number/Purchase order Number
D. Contract Type (e.g., FFP, T&M, LH, CR, etc.)
E. Total Contract Cost/Price
F. Period of Performance
G. Description of work performed
H. Valid name, phone number, and email address of CO and Contracting Officer's Representative (COR) or Program Manager (PM)

Quoter is advised that the Government may independently obtain and evaluate corporate experience data and/or verify actual accomplishment data. The burden of providing thorough and complete corporate experience information remains with the Quoter.

Quoters are expected to provide experience that is similar in size, scope and complexity to the SOW to be considered relevant under Factor 1.

**Prior Experience Questions (Factor 1) (2-pages max)**

**a)** What is your prior experience providing technical oversight, scientific review, and forensic toxicology inspection services for SAMHSA/DHHS or federally regulated post-accident toxicology testing laboratories? What is your experience designing and conducting laboratory and in-revenue field tests on active locomotive engines across varying environmental conditions?
**b)** What is your experience designing, implementing, and administering open proficiency testing programs involving spiked and blank whole blood and urine samples and managing reference laboratories?
**c)** What is your experience providing expert audit support, technical assistance, and compliance reviews for rail carriers and service providers under 49 CFR Part 219 and 49 CFR Part 40 regulations?

### 2.3.3 Volume 2: Factor 2 – Technical & Management Approach (Written Submission)

**Written Submission – Technical and Management Approach**

The Quoter shall provide their written quote in PDF and shall include the following:

This element shall consist of a narrative of the Quoter's technical and management approach to successfully accomplish the work required in the SOW. At a minimum, please include the following:

- Communication with internal/external stakeholders
- Handling conflicts or misalignments within the team or with clients
- Staff Departure Continuity / Backfills

In addition, the Quoter should address the following with their technical approach:

- A Detailed technical methodology for conducting tri-annual laboratory inspections, applying the four-tier rating system (In Compliance, Recommendations Offered, Deficiencies Noted, Discrepancies Identified), and drafting inspection reports within required timelines.
- Approach to designing and operating an open proficiency testing program using reference laboratories across the full range of FRA analytes.
- Strategy for delivering 24/7 extended-hour expert consultation, post-accident analytical result interpretations, and compliance review support.

- Quoters shall also demonstrate their ability to meet all schedule requirements across the Period of Performance.
- Available corporate resources and capabilities to successfully fulfill the requirements and deliverables outlined in the SOW.
- Any information the Quoter wishes to bring to the attention of the Government.

The Quoter shall submit one (1) electronic copy of no more than three (3) pages in a written PDF format.

The Quoter may include a table of contents. The table of contents is not included in the page count.

May include Assumptions – Quoters must indicate, in this section only, if any technical related assumptions have been made, conditions have been stipulated. If technical assumptions are not noted in this Volume and this section of the quote, it will be assumed that the Quoter's quotation reflects no technical assumptions for award, and the Quoter agrees to comply with all the terms and conditions set forth herein.

It is not the responsibility of the Government to seek out and identify assumptions, conditions or technical exceptions buried within the Quoter's quote. Accordingly, any technical related assumptions listed in any other volume or section shall be null and void.

**Volume 3: Factor 3 – Price Quotation**

Volume II shall contain the Quoter's price quote. The price quotation shall follow the template provided in Attachment 2 - Pricing Worksheet. Quoters are also encouraged to propose discounts and should clearly identify differences between their proposed prices and discounted prices.

Once the government determines the quoter that is the best-suited (i.e., the apparent successful quoter), the government reserves the right to communicate with only that quoter to address any remaining issues, if necessary, and finalize a purchase order with that quoter. These issues may include technical and price. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the government, the government reserves the right to communicate with the next best-suited quoter based on the original analysis and address any remaining issues.

Only vendors that have a valid UEI and registered in the System for Awards Management (SAM) shall be eligible to be awarded a contract from the federal government.

Interested Quoters are reminded that award can only be made to a Quoter who is registered in accordance with FAR 52.204-7, Alternate I System for Award Management.

## 2. Evaluation Criteria

Confidence Ratings evaluation technique will be utilized with the following ratings:

| **Confidence Ratings** | |
|---|---|
| **High Confidence** | The Government has high confidence that the Quoter understands the requirement, proposes a sound approach, and will be successful in performing the contract. |

| Confidence Ratings | |
|---|---|
| **Some Confidence** | The Government has some confidence that the Quoter understands the requirement, proposes an acceptable approach, and will be successful in performing the contract. |
| **Low Confidence** | The Government has low confidence that the Quoter understands the requirement, proposes an adequate approach, and will be successful in performing the contract. |

Please note, price will not be given a confidence rating.

### 3.1 Basis for Award

It is the Government's intent to award a purchase order to the quoter whose quote, in conforming to the RFQ, provides the overall best solution to the Government considering price and non-price factors. Evaluation and award will be conducted using the streamlined commercial procedures of FAR Part 12.

To be considered for award, Quoters must submit a full technical and price quote. The Government will utilize a best-value tradeoff process among the non-price and price factors to determine the optimal solution. Non-price factors (Factor 1 and 2), when combined, are significantly more important than price (Factor 3). However, price will become a more determining factor in the tradeoff analysis as technical ratings become closer.

The Government may reject any quote that is evaluated to be non-compliant with the RFQ requirements or reflects a failure to comprehend the complexity and risks of the work to be performed.

Should initial quotes not provide the Government with a satisfactory total solution, the Government reserves the right to engage with Quoters to obtain a better understanding and to reach a determination. The Government reserves the right to engage all, some, or none of the Quoters submitting quotations in response to this RFQ. Evaluations will be based solely on the information included in the quote. After receipt of quotations, the Government will conduct an evaluation. At any time prior to selection, including upon receipt of quotes, the Government may exclude a quote from further consideration for any material failure to follow instructions, including the omission of required information.

The government reserves the right to engage with only the apparent awardee to address any remaining issues, if necessary, and finalize a purchase order to that Quoter. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the government, the government reserves the right to engage other quoters based on the original analysis and address any remaining issues. This process will continue until an agreement is successfully reached and the resulting purchase order is awarded.

#### A. Non- Price Factors

- Factor 1 : Prior Experience

  The Government will evaluate the depth, breadth, and relevance of the Quoter's prior experience within the past five (5) years to assess the likelihood of successful performance under the SOW.

- Factor 2: Technical and Management Approach

  The Government will evaluate the Quoter's technical volume to assess the technical soundness, feasibility, and efficiency of the proposed technical and management approach in fulfilling the requirements of the SOW.

**B. Price**

- Factor 3: Price Quote (Firm Fixed Price)

The Government will evaluate the Quoter's Price Quote to ensure completeness, accuracy, and overall price reasonableness. Price will not receive a qualitative technical rating.

**3. Contract Clauses and Provisions**

**Provisions**

**52.212-1 Instructions to Offerors—Commercial Products and Commercial Services. (SEP 2023)**

**52.204-7 System for Award Management. (NOV 2024)**

**52.207-6 Solicitation of Offers from Small Business Concerns and Small Business Teaming Arrangements or Joint Ventures (Multiple-Award Contracts). (AUG 2024)**

**52.209-5 Certification Regarding Responsibility Matters. (AUG 2020)**

**52.209-7 Information Regarding Responsibility Matters. (OCT 2018)**

**52.209-11 Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law. (FEB 2016)**

**52.222-50 Combating Trafficking in Persons. (OCT 2025)**

**Clauses**

**FEDERAL ACQUISITION REGULATIONS**

**52.203-5 Covenant Against Contingent Fees. (MAY 2014)**

**52.203-7 Anti-Kickback Procedures. (JUN 2020)**

**52.203-16 Preventing Personal Conflicts of Interest (JUN 2020)**

**52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements. (JAN 2017)**

(a) Definitions. As used in this clause-

*Internal confidentiality agreement* or statement means a confidentiality agreement or any other written statement that the quoter requires any of its employees or subcontractors to sign regarding nondisclosure of quoter information, except that it does not include confidentiality agreements arising out of civil litigation or confidentiality agreements that contractor employees or subcontractors sign at the behest of a Federal agency.

*Subcontract* means any contract as defined in subpart 2.1 entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes but is not limited to purchase orders, and changes and modifications to purchase orders.

*Subcontractor* means any supplier, distributor, vendor, or Schedule Holder (including a consultant) that furnishes supplies or services to or for a prime contractor or another subcontractor.

(b) The Contractor shall not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(c) The Contractor shall notify current employees and subcontractors that prohibitions and restrictions of any preexisting internal confidentiality agreements or statements covered by this clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

(d) The prohibition in paragraph (b) of this clause does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(e) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235), and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions) use of funds appropriated (or otherwise made available) is prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(f) The Contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such contracts.

(End of clause)

**52.204-26 Covered Telecommunications Equipment or Services-Representation. (OCT 2020)**

**52.212-4 Contract Terms and Conditions - Commercial Products and Commercial Services, Alternate I. (NOV 2021)**

**52.217-8 Option to Extend Services (Nov 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but

the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor at any time prior to contract expiration.

(End of clause)

**52.217-9 Option to Extend the Term of the Contract (Mar 2000)**

(a) The Government may extend the term of this contract by written notice to the Contractor at any time prior to contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 1 day before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

(End of clause)

**52.222-43 Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts). (AUG 2018)**

**52.222-44 Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment. (MAY 2014)**

**52.222-90 Addressing DEI Discrimination by Federal Contractors.**

**FAR Class Deviation (CD) 2026-24**

**Addressing DEI Discrimination by Federal Contractors (APRIL 2026)**

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

*Program participation* means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

*Racially discriminatory diversity, equity, and inclusion (DEI) activities* means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (*e.g.*, vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

(1) The Contractor will not engage in any racially discriminatory DEI activities;
(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;
(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;

(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and

(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.

(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of clause)

**52.227-14 Rights in Data-General (MAY 2014)**

**52.232-1 Payment (APR 1984)**

**52.232-7 Payments under Time-and-Material and Labor-Hour Contract (NOV 2021)**

**52.232-8 Discounts for Prompt Payment (FEB 2002)**

**52.232-18 Availability of Funds (APR 1984)**

**52.232-22 Limitation of Funds (APR 1984)**

**52.242-15 Stop-Work Order (AUG 1989)**

**52.246-4 Inspection of Services - Fixed-Price. (AUG 1996)**

**52.246-6 Inspection - Time-and-Material and Labor-Hour. (MAY 2001)**

**52.249-14 Excusable Delays (APR 1984)**

**52.252-2 Clauses Incorporated by Reference. (FEB 1998)**

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov

(End of clause)

**TRANSPORTATION ACQUISITION REGULATIONS**

**1252.201-70 Contracting Officer's Representative (NOV 2022)**

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Representative (COR) to perform functions under the contract such as review and/or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COR under the contract.

(b) The Contracting Officer cannot authorize the COR or any other representative to sign documents (*i.e.,* contracts, contract modifications, etc.) that require the signature of the Contracting Officer.

(End of clause)

**1252.204-70 Contractor Personnel Security and Agency Access (NOV 2022)**

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

*Agency access* means access to DOT facilities, sensitive information, information systems or other DOT resources.

*Applicant* means a contractor employee for whom the Contractor applies for a DOT identification card.

*Contractor employee* means a prime contractor and subcontractor employee who requires agency access to perform work under a DOT contract.

*Identification card (or "ID card")* means a government issued or accepted identification card such as a Personal Identity Verification (PIV) card, a PIV-Interoperable (PIV-I) card from an authorized PIV-1 issuer, or a non-PIV card issued by DOT, or a nonPIV card issued by another Federal agency and approved by DOT. PIV and PIV-1 cards have physical and electronic attributes that other (non-PIV) ID cards do not have.

*Issuing office* means the DOT entity that issues identification cards to contractor employees.

*Local security servicing organization* means the DOT entity that provides security services to the DOT organization sponsoring the contract.

(b) *Risk and sensitivity level designations.* For contracts requiring access to DOT facilities, sensitive information, information systems or other DOT resources, contractor employees will be required to complete background investigations, identity proofing, and government identification card application procedures to determine suitability for access. DOT will assign a risk and sensitivity level designation to the overall contract and/or to contractor employee positions by category, group or individual. The risk and sensitivity level designations will be the basis for determining the level of personnel security processing required for contractor employees. The following risk and sensitivity level designations and associated level of processing are required, and each level includes the prior levels -

(1) Low risk level: National Agency Check with Written Inquiries (NACI);

(2) Moderate risk level: Minimum Background Investigation (MBI); and

(3) High risk level: Background Investigation.

(c) *Security clearances.* Contractor employees may also 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) *Pre-screening of contractor employees.* The Contractor must pre-screen individuals designated for employment under any DOT contract by verifying minimal suitability requirements to ensure that only candidates that appear to meet such requirements are considered for contract employment, and to mitigate the burden on the Government of conducting background investigations on objectionable applicants. The Contractor must exercise due diligence in pre-screening all employees prior to submission to DOT for agency access. DOT may decline to grant agency access to a contractor employee for reasons including, but not limited to -

(1) Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude;

(2) Falsification of information entered on forms or of other documents submitted;

(3) Improper conduct including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct adverse to the Government regardless of whether the conduct is directly related to the contract; and

(4) Any behavior judged to pose a potential threat to DOT facilities, sensitive information, information systems or other resources.

(e) *Citizenship status.* The Contractor must monitor a non-citizen's continued authorization for employment in the United States. The Contractor must provide documentation to the Contracting Officer or the Contracting Officer's Representative (COR) during the background investigation process that validates that the E-Verify requirement has been met for each contractor employee.

(f) *Background investigation and adjudication.* A contractor employee must have a favorable adjudication of background investigation before DOT will issue an ID card to the contractor employee granting access to DOT facilities, sensitive information, information systems or other DOT resources. DOT may accept favorable adjudications of background investigations from other Federal agencies when applicants have held PIV cards issued by those agencies with no break in service. DOT may also accept PIV-I (Interoperable) cards issued by an authorized PIV-1 issuer as evidence of identity. A favorable adjudication does not preclude DOT from initiating a new investigation when deemed necessary. At a minimum, the FBI National Criminal History Check (fingerprint check) must be favorably completed before a DOT identification card can be issued. Each Contractor must use the Office of Personnel Management's (OPM) e-QIP system to complete any required investigative forms. Instructions for obtaining fingerprints will be provided by the COR or Contracting Officer. The DOT Office of Security, M-40, or a DOT organization delegated authority by M-40, is responsible for adjudicating the suitability of contractor employees.

(g) *Agency access denied.* Upon contract award, DOT will initiate the agency access procedure for all contractor employees requiring access to DOT facilities, sensitive information, information systems and other DOT resources for contract performance. DOT may deny agency access to any individual about whom an adverse suitability determination is made. Failure to submit the required security information or to truthfully answer all questions shall constitute grounds for denial of access. The Contractor must not provide agency access to contractor employees until the COR or Contracting Officer provides notice of approval, which is authorized only by the DOT Office of Security (M-40), or a DOT organization delegated authority by M-40. Where a proposed contractor employee is denied agency access by the Government or, if for any reason a proposed application is withdrawn by the

Contractor during the agency access process, the additional costs and administrative burden for conducting additional background investigations caused by a lack of effective prescreening or planning on the part of the Contractor may be considered as part of the Contractor's overall performance evaluation.

(h) *Identification card application process.* The COR will be the DOT ID card Sponsor and point of contact for the Contractor's application for a DOT ID card. The COR shall review and approve the DOT ID card application before an ID card is issued to the applicant. An applicant may be issued either a Personal Identity Verification (PIV) card that meets the standards of Homeland Presidential Security Directive (HSPD-12), or an applicant may be issued a non-PIV card. Generally, a non-PIV card will be issued for contracts that expire in six months or less, including option periods. The COR may request the issuing office to waive the six-month eligibility requirement when it is in DOT's interest for contract performance. The following applies -

(1) PIV card. The applicant must complete a DOT on-line application for a PIV card;

(2) Non-PIV card. The applicant must complete and submit a hard copy of Form 1681 to the COR/Sponsor; and

(3) Regardless of the type of card to be issued (PIV or non-PIV), the applicant must appear in person to provide two forms of identity source documents in original form to DOT. The identity source documents must come from the list of acceptable documents included in Form F-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document must be a valid State or Federal government-issued picture identification. For a PIV card, the applicant may be required to appear in-person a second time for enrollment and activation.

(i) *Identification card custody and control.* The Contractor is responsible for the custody and control of all forms of government identification issued by DOT to contractor employees for access to DOT facilities, sensitive information, information systems and other DOT resources. The Contractor shall:

(1) Provide a listing of personnel for whom an identification (ID) card is requested to the COR or PM who will provide a copy of the listing to the card issuing office. This may include Contractor and subcontractor personnel. Follow issuing office directions for submittal of an application package(s).

(2) While visiting or performing work on a DOT facility, as specified by the issuing office, PM or COR, ensure that contractor employees prominently display their ID card.

(3) Immediately notify the COR or, if the COR is unavailable, the Contracting Officer when a contractor employee's status changes and no longer requires agency access (*e.g.,* employee's transfer, completion of a project, retirement, removal from work on the contract, or termination of employment) that may affect the employee's eligibility for access to the facility, sensitive information, or resources.

(4) Promptly deliver to the issuing office: (a) all ID cards assigned to an employee who no longer requires access to the facility; and (b) all expired ID cards within five (5) days of their expiration or all cards at time of contract termination, whichever occurs first.

(5) Immediately report any lost or stolen ID cards to the issuing office and follow its instructions.

(i) The Contractor is responsible for maintaining and safeguarding the DOT ID card upon issuance to the contractor employee. The Contractor must ensure that contractor employees comply with DOT requirements concerning the renewal, loss, theft, or damage of an ID card. The Contractor must immediately notify the COR or, if the COR is unavailable, the Contracting Officer when an ID card is lost, stolen or damaged.

(ii) Failure to comply with the requirements for custody and control of DOT ID cards may result in withholding final payment or contract termination based on the potential for serious harm caused by inappropriate access to DOT facilities, sensitive information, information systems or other DOT resources.

(iii) Specific actions and activities are required in certain events -

(A) Renewal. A contractor employee's DOT issued ID card is valid for a maximum of three years or until the contract expiration date (including option periods), whichever occurs first. The renewal process should begin six weeks before the PIV card expiration date. If a PIV card is not renewed before it expires, the contractor employee will be required to sign-in daily for facility access and may have limited access to information systems and other resources.

(B) Lost/stolen. Immediately upon detection, the Contractor or contractor employee must report a lost or stolen DOT ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local servicing security organization. The Contractor must submit an incident report within 48 hours, through the COR or, if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization describing the circumstances of the loss or theft. The Contractor must also report a lost or stolen PIV card through the DOT on-line registration system. If the loss or theft is reported by the Contractor to the local police, a copy of the police report must be provided to the COR or Contracting Officer. From the date of notification to DOT, the Contractor must wait three days before getting a replacement ID card. During the 3-day wait period, the contractor employee must sign in daily for facility access.

(C) Replacement. An ID card will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than 3 days, provided there is a continuing need for agency access to perform work under the contract.

(D) Surrender of ID cards. Upon notification that routine access to DOT facilities, sensitive information, information systems or other DOT resources is no longer required, the Contractor must surrender the DOT issued ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization in accordance with agency procedures.

(j) *Flow down of clause.* The Contractor is required to include this clause in any subcontracts at any tier that require the subcontractor or subcontractor's employees to have access to DOT facilities, sensitive information, information systems or other resources.

(End of clause)

**1252.209-70 Organizational and Consultant Conflicts of Interest (NOV 2022)**

(a) An Quoter shall identify in its proposal, quote, bid or any resulting contract, any potential or actual Organizational and Consultant Conflicts of Interest (OCCI) as described in FAR subpart 9.5. This includes actual or potential conflicts of interests of proposed subcontractors. If a Quoter

identifies in its proposal, quote, bid or any resulting contract, a potential or actual conflict of interests the Quoter shall submit an Organizational and Consultant Conflicts of Interest Plan (OCCIP) to the contracting officer. The OCCIP shall describe how the Quoter addresses potential or actual conflicts of interest and identify how they will avoid, neutralize, or mitigate present or future conflicts of interest.

(b) Quoters must consider whether their involvement and participation raises any OCCI issues, especially in the following areas when:

(1) Providing systems engineering and technical direction.

(2) Preparing specifications or work statements and/or objectives.

(3) Providing evaluation services.

(4) Obtaining access to proprietary information.

(c) If a prime contractor or subcontractor breaches any of the OCCI restrictions or does not disclose or misrepresents any relevant facts concerning its conflict of interest, the government may take appropriate action, including terminating the contract, in addition to any remedies that may be otherwise permitted by the contract or operation of law.

(End of clause)

**1252.217-74 Subcontracts (NOV 2022)**

**1252.222-70 Strikes or Picketing Affecting Timely Completion of the Contract Work (NOV 2022)**

**1252.223-73 Seat Belt Use Policies and Programs (NOV 2022)**

In accordance with Executive Order 13043, Increasing Seat Belt Use in the United States, dated April 16, 1997, the Contractor is encouraged to adopt and enforce on-the-job seat belt use policies and programs for its employees when operating company-owned, rented, or personally-owned vehicles. The National Highway Traffic Safety Administration (NHTSA) is responsible for providing leadership and guidance in support of this Presidential initiative. For information on how to implement such a program or for statistics on the potential benefits and cost-savings to your company or organization, please visit the Click it or Ticket seat belt safety section of NHTSA's website at *https://www.nhtsa.gov/campaign/click-it-or-ticket* and *https://www.nhtsa.gov/risky-driving/seat-belts.*

(End of clause)

**1252.232-70 Electronic Submission of Payment Requests (NOV 2022)**

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

(1) *Contract financing payment* has the meaning given in FAR 32.001.

(2) *Payment request* means a bill, voucher, invoice, or request for contract financing payment or invoice payment with associated supporting documentation. The payment request must comply with the requirements identified in FAR 32.905(b), "Content of Invoices," this clause, and the applicable Payment clause included in this contract.

(3) *Electronic form* means an automated system transmitting information electronically according to the accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, email, and scanned documents are not acceptable electronic forms for submission of payment requests.

(4) *Invoice payment* has the meaning given in FAR 32.001.

(b) *Electronic payment requests.* Except as provided in paragraph (e) of this clause, the contractor shall submit payment requests in electronic form. Purchases paid with a Governmentwide commercial purchase card are considered to be an electronic transaction for purposes of this rule, and therefore no additional electronic invoice submission is required.

(c) *Processing system.* The Department of Transportation utilizes the DELPHI system for processing invoices. The DELPHI module for submitting invoices is called *iSupplier.* Access to DELPHI is granted with electronic authentication of credentials (name & valid email address) utilizing the GSA credentialing platform *login.gov.* Vendors submitting invoices are required to submit invoices via *iSupplier* (DELPHI) and authenticated via *www.login.gov.*

(d) *Invoice requirements.* To receive payment and in accordance with the Prompt Payment Act, all invoices submitted as attachments in *iSupplier* (DELPHI) shall contain the following:

(1) Invoice number and invoice date.

(2) Period of performance covered by invoice.

(3) Contract number and title.

(4) Task/Delivery Order number and title (if applicable).

(5) Amount billed (by CLIN), current and cumulative.

(6) Total ($) of billing.

(7) Cumulative total billed for all contract work to date.

(8) Name, title, phone number, and mailing address of person to be contacted in the event of a defective invoice.

(9) Travel. If the contract includes allowances for travel, all invoices which include charges pertaining to travel expenses will catalog a breakdown of reimbursable expenses with the appropriate receipts to substantiate the travel expenses.

**(TAR Class Deviation 2025-02_A1)**

(10) The Contractor certifies that, by submitting this invoice to the Government, the supplies and/or services billed have been shipped, rendered, or delivered in accordance with instructions issued by the ordering officer; that they are reflected in the quantities and/or period of performance stated on the invoice; and that such supplies and/or services conform to the quantity and quality requirements specified in the applicable contract, order, or blanket purchase agreement.

Furthermore, pursuant to Executive Order 14173, Ending Illegal Discrimination And Restoring Merit-Based Opportunity, the Contractor certifies that it is in compliance with the Equal Protection principles of the Constitution and all applicable Federal anti-discrimination laws, and acknowledges that such compliance is material to the Government's payment decision under the False Claims Act (31 U.S.C. § 3729(b)(4)). The Contractor also affirms that it does not operate any diversity, equity, and inclusion (DEI) initiatives that are inconsistent with the Equal Protection principles of the Constitution and the non-discrimination requirements of Federal law, as interpreted by the Supreme Court in Students for Fair Admissions v. Harvard, 600 U.S. 181 (2023).

(e) *Payment system registration.* All persons accessing the *iSupplier* (DELPHI) will be required to have their own unique user ID and password and be credentialed through *login.gov.*

(1) *Electronic authentication. See www.login.gov* for instructions.

(2) To create a *www.login.gov* account, the user will need a valid email address and a working phone number. The user will create a password and then *www.login.gov* will reply with an email confirming the email address.

(3) *iSupplier* (DELPHI) registration instructions: New users should navigate to: *http://einvoice.esc.gov* to establish an account. Users are required to log in to *iSupplier* (DELPHI) every 45 days to keep it active.

(4) *Training on DELPHI.* To facilitate use of DELPHI, comprehensive user information is available at *http://einvoice.esc.gov.*

(5) *Account Management.* Vendors are responsible to contact their assigned COR when their firm's points of contact will no longer be submitting invoices, so they can be removed from the system.

(f) *Waivers.* For contractors/vendors who are unable to utilize DOT's DELPHI system, waivers may be considered by DOT on a case-by-case basis. Vendors should contact their Contracting Officer's Representative (COR) for procedures.

(g) *Exceptions and alternate payment procedures.* If, based on one of the circumstances set forth in 1232.7002(a) or (b), and the contracting officer directs that payment requests be made by mail, the contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. If alternate payment procedures are authorized, the Contractor shall include a copy of the Contracting Officer's written authorization with each payment request. If DELPHI is succeeded by later technology, the Contracting Officer will supply the Contractor with the latest applicable electronic invoicing instructions.

(End of clause)

**1252.237-70 Qualifications of Contractor Employees (Nov 2022)**

(a) *Definition. Sensitive information,* as used in this clause, means any information that is proprietary data or, if subject to unauthorized access, modification, loss, or misuse, could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals specified in The Privacy Act, 5 U.S.C. 552a, but has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

(b) Work under this contract may involve access to DOT facilities or sensitive information or resources (*e.g.,* information technology including computer systems). To protect sensitive information, which shall not be disclosed by the contractor unless authorized in writing by the Contracting Officer, the Contractor shall provide training to any contractor employees authorized to access sensitive information, and upon request of the Government, provide information to assist the Government in determining an individual's suitability to have authorization.

(c) The Contracting Officer may require dismissal from work under this contract of those employees deemed incompetent, careless, insubordinate, unsuitable, or otherwise objectionable, or whose continued employment is deemed contrary to the public interest or inconsistent with the best interest of national security.

(d) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's Representative (COR) or Program Manager's (PM) request, the Contractor's employees shall be fingerprinted or subject to other investigations as required.

(e) The Contractor shall ensure that contractor employees working on this contract are citizens of the United States of America or non-citizens who have been lawfully admitted for permanent residence or employment (indicated by immigration status) as evidenced by U.S. Citizenship and Immigration Services (USCIS) documentation.

(f) Subcontract flow-down requirement. The Contractor shall include this clause, including this paragraph (f), in subcontracts whenever this clause is included in the prime contractor's contract.

(End of clause)

**1252.239-70 Security Requirements for Unclassified Information Technology Resources (NOV 2022)**

(a) The Contractor shall be responsible for information technology security for all systems connected to a Department of Transportation (DOT) network or operated by the Contractor for DOT, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to DOT information that directly supports the mission of DOT. The term “information technology,” as used in this clause, means any equipment or interconnected system or subsystem of equipment, including telecommunications equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data

or information. This includes both major applications and general support systems as defined by OMB Circular A–130. Examples of tasks that require security provisions include—

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

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

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

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

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

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

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

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

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

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

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

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

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

(g) The Contractor shall 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.

(h) The Contractor shall ensure that its employees performing services under this contract receive annual IT security training in accordance with OMB Circular A–130, FISMA, and NIST requirements, as amended, with a specific emphasis on rules of behavior.

(i) 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 shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

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

(End of clause)

**1252.239-73 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information. (NOV 2022)**

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

*Compromise* means disclosure of information to unauthorized persons, or a violation of the security policy of a system, whereby without authorization information is disclosed, modified, destroyed, lost, or copied to unauthorized media-whether intentionally or unintentionally.

*DOT sensitive data* means unclassified information that requires safeguarding, or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is-

(1) Marked or otherwise identified in the contract, purchase order, or delivery order and provided to the Contractor by or on behalf of DOT in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the Contractor in support of the performance of the contract.
*Cyber incident* means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

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

*Media* means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which DOT sensitive data is recorded, stored, or printed within a covered contractor information system.

*DOT technical information* means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Restrictions*. (1) The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract derived from a third-party's reporting of a cyber incident, pursuant to TAR clause, 1252.239-74, Safeguarding DOT Sensitive Data and Cyber Incident Reporting (or derived from such information obtained under that clause):

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

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

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

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

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

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

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

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

(End of clause)

**1252.239-74 Safeguarding DOT Sensitive Data and Cyber Incident Reporting. (NOV 2022)**

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

*Adequate security* means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information against the probability of occurrence.

*Compromise* means disclosure of information to unauthorized persons, or a violation of the security policy of a system, whereby without authorization information is disclosed, modified, destroyed, lost, or copied to unauthorized media-whether intentionally or unintentionally.

*Contractor attributional/proprietary information* means information that identifies the Contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the Contractor(s) (*e.g*., program description, facility locations), personally identifiable information, trade secrets, commercial or financial information, or other commercially sensitive information not customarily shared outside of a company.

*Covered contractor information system* means an unclassified information system owned or operated by or for a Contractor and that processes, stores, or transmits DOT sensitive data.

*DOT sensitive data* means unclassified information that requires safeguarding, or dissemination controls pursuant to and consistent with law, regulation, and Government-wide policies, and is-

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the Contractor by or on behalf of DOT in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the Contractor in support of the performance of the contract.

*Cyber incident* means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

*Federal record* as defined in 44 U.S.C. 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. The term Federal record-

(1) Includes all DOT records;

(2) Does not include personal materials;

(3) Applies to records created, received, or maintained by Contractors pursuant to a DOT contract; and

(4) May include deliverables and documentation associated with deliverables.

*Forensic analysis* means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

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

*Malicious software* means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

*Media* means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts

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

*Operationally critical support* means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

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

*Technical information* means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered Contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 1252.239-76, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (*i.e*., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered Contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(iv) of this clause, the contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 2, "Protecting Controlled

Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at *https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final*) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii) The Contractor shall implement NIST SP 800-171, Rev. 2, no later than 30 days after the award of this contract. The Contractor shall notify Contract Officer of any security requirements specified by NIST SP 800-171, Rev. 2 not implemented within 30 days of time of contract award.
(iii) If the Vendor 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 Vendor 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 Vendor requests to vary from NIST SP 800-171, Rev. 2 requirements and inform the Vendor in writing of its decision before contract award. The Government will incorporate accepted variance(s) from NIST SP 800-171, Rev. 2 into any resulting contract.

(v) The Contractor need not implement any security requirement adjudicated by an authorized representative of the DOT CIO to be nonapplicable, or have an alternative, but equally effective, security measure that may be implemented in its place.

(vi) If the DOT CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when the Contractor requests its recognition under this contract

(3) If the Contractor intends to use an external cloud service provider to store, process, or transmit any DOT sensitive data in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (*https://www.fedramp.gov/resources/documents/*) and that the cloud service provider complies with requirements in paragraphs (c) through (h) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(4) The Contractor will apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (b)(2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (*e.g.*, medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan, as required by, clause 1252.239-70, Security Requirements for Unclassified Information Technology Resources.

(c) *Cyber incident reporting requirement*. (1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the DOT sensitive data residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall-

(i) Conduct a review for evidence of compromise of DOT sensitive data, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised DOT sensitive data or whether the incident affects the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DOT Security Operations Center (SOC) 24x7x365 at phone number: 571-209-3080 (Toll Free: 1-866-580-1852).

(d) *Cyber incident report*. The cyber incident report shall be treated as information created by or for DOT and shall include, at a minimum, the required elements in paragraph (c)(1)(i).

(e) *Spillage*. Upon notification by the Government of a spillage, or upon the Contractor's discovery of a spillage, the Contractor shall cooperate with the Contracting Officer to address the spillage in compliance with DOT policy.

(f) *Malicious software*. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, the Contractor shall submit the malicious software to DOT in accordance with instructions provided by the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(g) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DOT to request the media or decline interest.

(h) *Access to additional information or equipment necessary for forensic analysis*. Upon request by DOT, the Contractor shall provide DOT with access to additional information or equipment that is necessary to conduct a forensic analysis.

(i) *Cyber incident damage assessment activities*. If DOT elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (c) of this clause.

(j) *DOT safeguarding and use of Contractor attributional/proprietary information*. The Government shall protect against the unauthorized use or release of information obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that includes Contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the Contractor attributional/proprietary information that is included in such authorized release consistent with applicable law.

(k) *Use and release of Contractor attributional/proprietary information not created by or for DOT*. Information that is obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that is not created by or for DOT is authorized to be released outside of DOT-

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 1252.239-73, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information; or

(5) With Contractor's consent; or

(6) As otherwise required by law.

(l) *Use and release of Contractor attributional/proprietary information created by or for DOT*. Information that is obtained from the Contractor (or derived from information obtained from the Contractor) under this clause that is created by or for DOT (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DOT for purposes and activities authorized by paragraph (j)

of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(m) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(n) *Other safeguarding or reporting requirements*. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable Government statutory or regulatory requirements.

(o) *Subcontract flowdown requirements*. The Contractor shall-

(1) Include this clause, including this paragraph (o), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve DOT sensitive data, including subcontracts for commercial products and commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as DOT sensitive data and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to-

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171, Rev. 2 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(iii) of this clause; and

(ii) Provide the incident report number, automatically assigned by DOT, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DOT as required in paragraph (c) of this clause.

(End of clause)

**1252.239-91 Records Management. (NOV 2022)**

(a) *Definition*.

*Federal record*, as defined in 44 U.S.C. 3301, means all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. The term Federal record:

(1) Includes all DOT records.

(2) Does not include personal materials.

(3) Applies to records created, received, or maintained by Contractors pursuant to a DOT contract.

(4) May include deliverables and documentation associated with deliverables.

(b) *Requirements*. (1) *Compliance*. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to 44 U.S.C. chapters 21, 29, 31, and 33, NARA regulations at 36 CFR chapter XII, subchapter B, and those policies associated with the safeguarding of records covered by Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

(2) *Applicability*. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under, the legal control of the Government, are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended. Such Federal records shall be managed and scheduled for disposition only as permitted by the Federal Records Act, other relevant statutes or regulations, and DOT Order 1351.28, Departmental Records Management Policy.

(3) *Records maintenance*. While DOT records are in the Contractor's custody, the Contractor is responsible for preventing the alienation or unauthorized destruction of DOT records, including all forms of mutilation. Records may not be removed from the legal custody of DOT or destroyed except in accordance with the provisions of the agency records schedules and with the written concurrence of the DOT or Component Records Officer, as appropriate. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, the Contractor must report the event to the Contracting Officer in accordance with 36 CFR part 1230, Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records, for reporting to NARA.

(4) *Unauthorized disclosure*. The Contractor shall notify the Contracting Officer within two hours of discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment. The Contractor shall not remove material from Government facilities or systems, or facilities or systems

operated or maintained on the Government's behalf, without the express written permission of the Contracting Officer. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to DOT control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the contract. Destruction of records is expressly prohibited unless in accordance with the contract.

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

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

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

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

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

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

(End of clause)

**1252.242-71 Contractor Testimony (NOV 2022)**

All requests for the testimony of the Contractor or its employees, and any intention to testify as an expert witness relating to: (a) any work required by, and/or performed under, this contract; or (b) any information provided by any party to assist the Contractor in the performance of this contract, shall be

immediately reported to the Contracting Officer. Neither the Contractor nor its employees shall testify on a matter related to work performed or information provided under this contract, either voluntarily or pursuant to a request, in any judicial or administrative proceeding unless approved, in advance, by the Contracting Officer or required by a judge in a final court order.

(End of clause)

**1252.242-72 Dissemination of Contract Information (NOV 2022)**

The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. Two copies of any material proposed to be published or distributed shall be submitted to the Contracting Officer.

(End of clause)

**1252.245-70 – Use of Government Furnished Equipment or Information —Official, Unofficial, and Personal International Travel (MAR 2024) (DEVIATION)**

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

(End of clause)

## 4. Attachments

1. **Statement of Work**
2. **Pricing Worksheet**