1252.239-75 DOT Protection of Information About Individuals, PII, and Privacy Risk Management Requirements.

As prescribed in 1239.7104, insert the following clause:

DOT PROTECTION OF INFORMATION ABOUT INDIVIDUALS, PII, AND PRIVACY RISK MANAGEMENT REQUIREMENTS (DATE)

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

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

(c) *Privacy Act.* The Contractor will –

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

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

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

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

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

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

(g) *NIST FIPS 140-2.* At a minimum, the Contractor shall protect all PII created, collected, used, maintained, or disseminated on behalf of the Department using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards, unless otherwise authorized by the DOT Chief Privacy Officer.

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

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

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

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

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

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

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

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

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

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

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

(End of clause)