<?xml encoding="UTF-8">

Subpart 1239.71—Protection of Data About Individuals

Parent topic: PART 1239—ACQUISITION OF INFORMATION TECHNOLOGY

1239.7100 Scope of subpart.

This subpart includes Privacy Act and data protection considerations for DOT contracts. Data protection requirements are in addition to provisions concerning the general protection of individual privacy (*see* FAR subpart 24.1) and privacy in the acquisition of information technology (*see* FAR 39.105). DOT rules and regulations implementing the Privacy Act of 1974 are located at 49 CFR part 10.

1239.7101 Definitions.

As used in this subpart—

Breach means the disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized access, compromise, use, disclosure, modification, destruction, access or loss use of data, or the copying of information to unauthorized media may have occurred.

Data protection means the practice of protecting data and managing risks associated with the collection, display, use, processing, storage, transmission, and disposal of information or data as well as the systems and processes used for those purposes. Data protection uses physical, technical, and administrative controls to protect the integrity, availability, authenticity, non-repudiation, and confidentiality of data by incorporating protection, detection, and reaction capabilities. Data protection encompasses not only digital data, but also data in analog or physical form, and applies to data in transit as well as data at rest.

Information security means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) *Integrity,* which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(2) *Confidentiality,* which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) *Availability,* which means ensuring timely and reliable access to and use of information.

Personally Identifiable Information (PII) means the definition as set forth in FAR 24.101.

Privacy incident means the loss of control, compromise, unauthorized disclosure, unauthorized

acquisition, or unauthorized access to PII regardless of format.

1239.7102 Policy.

DOT must ensure that data protection is provided for information and information systems in accordance with current policies, procedures, and statutes, including:

(a) The Clinger-Cohen Act.

(b) The E-Government Act.

(c) Federal Information Systems Modernization Act.

(d) Federal Information Processing Standards.

(e) OMB Circular A–130, Managing Information as a Strategic Resource.

(f) 49 CFR part 10, Maintenance of and Access to Records Pertaining to Individuals.

(g) DOT Order 1351.18, Privacy Risk Management Policy.

(h) DOT Order 1351.19, PII Breach Notification Controls.

(i) DOT Order 1351.28, Records Management.

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

1239.7103 Responsibilities.

(a) The contracting officer will include appropriate data protection requirements in all contracts and other acquisition-related documents for DOT information created, collected, displayed, used, processed, stored, transmitted, and disposed of by contractors.

(b) The contracting officer will ensure all contracts with contractors maintaining information systems containing PII contain the appropriate clauses as may be required by the Federal Acquisition Regulation (FAR) and other OMB and agency memorandums and directives, to ensure that PII under the control of the contractor is maintained in accordance with Federal law and DOT policy.

(c) The contracting officer and assigned contracting officer's representatives and program and project managers will obtain contractual assurances from third parties working on official DOT business that third parties will protect PII in a manner consistent with the privacy practices of the Department during all phases of the system development lifecycle.

(d) Program and project managers and requiring activities will address the need to protect information about individuals and/or PII in the statement of work (SOW), performance work statement (PWS) or statement of objectives (SOO). Contracting officers will notify the appropriate organization or office when it intends to issue a solicitation for items or services requiring access to personal information or PII. Contracting officers will identify the Component Privacy Officer as the

point of contact for oversight of privacy protection and identify the Component Information Systems Security Manager for the component for oversight of information security to the contractor after award.

(e) See 1252.239–75, DOT Protection of Information about Individuals, PII and Privacy Risk Management Requirements, for additional information regarding the requirements of DOT Order 1351.18, Privacy Risk Management Policy and DOT Order 1351.37, Departmental Cyber Security Policy.

1239.7104 Contract clause.

The contracting officer shall insert the clause at 1252.239–75, DOT Protection of Information About Individuals, PII and Privacy Risk Management Requirements, in solicitations and contracts involving contractor performance of data protection functions and for contracts involving the design, development, or operation of an information system with access to personally identifiable information as described in DOT Order 1351.18, Privacy Risk Management, and DOT Order 1351.37, Departmental Cyber Security Policy.