

CIOP Chapter 38

DOT Privacy Policy for the Information Sharing Environment (ISE)

TABLE OF CONTENTS

Section 38.1	Purpose.....	1
Section 38.2	Background.....	1
Section 38.3	Scope and Applicability.....	2
Section 38.4	Policy	2
Section 38.5	Roles and Responsibilities	9
Section 38.6	Dates	10
Section 38.7	Cancellations.....	10
Section 38.8	Compliance	10
Section 38.9	Waivers	10
Section 38.10	Audit Procedures.....	10
Section 38.11	Approval	11
Appendix A	Glossary	A-1
Appendix B	Authorities.....	B-1

Section 38.1 Purpose

The DOT Privacy Policy for the Information Sharing Environment establishes policies and procedures and assigns responsibilities for collecting, using, storing, sharing, and securing terrorism-related Protected Information (PI) shared through the Information Sharing Environment (ISE), as required by the *Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines).¹ Protected Information refers to “information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States.”

(Table of Contents)

Section 38.2 Background

38.2.1 The ISE, in accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), provides analysts, operators, and investigators with integrated and synthesized terrorism, weapons of mass destruction, and homeland security information needed to enhance national security and help keep our people safe.

38.2.2 These analysts, operators, and investigators come from a variety of communities - law enforcement, public safety, homeland security, intelligence, defense, and foreign affairs – and may work for federal, state, local, tribal, or territorial governments. They also have mission needs to collaborate and share information with each other and with private sector partners and our foreign allies. While they work in different disciplines and have varying roles and responsibilities, they all rely on timely and accurate information to achieve their mission responsibilities.

38.2.3 The Program Manager for the ISE (ISE-PM) issued the ISE Privacy Guidelines and compliance with the ISE Privacy Guidelines is a prerequisite for participation in the ISE.

38.2.3.1 Agencies participating in the ISE must adopt a written privacy, civil rights, and civil liberties policy that is at least as comprehensive as the protection standards promulgated by the PM-ISE in the ISE Privacy Guidelines. This policy addresses that requirement.

(Table of Contents)

¹ The ISE Privacy Guidelines were developed by the Attorney General and the Director of National Intelligence pursuant to the President’s Memorandum of December 16, 2005. The ISE Privacy Guidelines were approved by the President and issued by the ISE Program Manager on December 4, 2006. See <http://ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf>

Section 38.3 Scope and Applicability

38.3.1 This Policy applies to all DOT activities related to the collection, use, storage, or sharing (dissemination) of terrorism-related PI in the ISE.

38.3.2 In addition, DOT has instituted a policy whereby any Personally Identifiable Information (PII) collected, used, maintained, or disseminated in connection with a mixed² system is treated as a system of records subject to the administrative, but not statutory, protections of the Privacy Act regardless of whether the information pertains to a U.S. citizen, lawful permanent resident, visitor, or alien. As a result, DOT, to the extent practicable, will extend the provisions of this Policy to PII about all individuals contained in its mixed systems, irrespective of whether that information is PI.

38.3.3 This Policy incorporates the statutory and regulatory standards with which DOT is required to comply, plus best practices that DOT has determined are important in providing adequate protection to the PI that DOT collects, uses, shares, and stores in the ISE.

Goal

38.3.4 The goal of this Policy is to facilitate the collection and use of PI to achieve the lawful purposes for which the data were collected and to meet DOT's responsibilities in delivering efficient, accessible, and convenient transportation systems and services while protecting the privacy, civil rights, and civil liberties of U.S. citizens and lawful permanent residents.

(Table of Contents)

Section 38.4 Policy

38.4.1 DOT maintains high standards for the protection of PI shared through the ISE. All Departmental elements will comply with the Constitution, applicable laws, regulations, Executive Orders, Office of Management and Budget (OMB) requirements and guidance, and other pertinent policies and guidelines relating to PI. This Policy outlines major requirements and provides a list of links to those requirements in the references section.

Collection (Acquisition and Access)

38.4.2 PI will be collected lawfully, and will be limited to those data that are required to complete transaction(s) relevant to DOT's mission. DOT has adopted internal policies and procedures requiring it to seek or retain only PI that is legally permissible for it to seek or retain under applicable statutes, regulations, policies, and Executive Orders. All information collected

² As used in this Policy, 'mixed' means a dataset that contains information about individuals who are protected by the Privacy Act (U.S. citizens and legal permanent residents) and individuals who are not (foreign citizens). DOT cannot extend the Privacy Act's statutory protections to individuals who are not protected by the Privacy Act, but DOT does extend the Act's administrative protections to these individuals.

will be used only for the purpose for which it was collected, unless authorized by law. Prior to beginning a new or modified information collection effort, all DOT elements will assess information collection practices to verify that:

- 38.4.2.1 Data collection is limited to what is essential to DOT's mission.
- 38.4.2.2 DOT received approval from OMB for the collection, in compliance with the Paperwork Reduction Act, if applicable.³
- 38.4.2.3 To the greatest extent possible, information is collected directly from the individual about whom it is collected.
- 38.4.2.4 The DOT element Privacy Officer has been notified of the information collection.
- 38.4.2.5 A Privacy Impact Assessment (PIA) has been conducted, if it is required for the information collection. A PIA is required:
 - 38.4.2.5.1 Prior to developing or procuring new technology that collects, maintains, or distributes personal information.
 - 38.4.2.5.2 Prior to initiating an electronic information collection effort from 10 or more members of the public.
 - 38.4.2.5.3 When making significant changes to an information system that creates new privacy risks for the information.
 - 38.4.2.5.4 For all rulemakings that have an impact on the privacy of the individuals affected by the rule.

Notice Mechanisms

38.4.3 DOT elements and information system owners ("system owners") participating in the ISE will establish notice mechanisms for communicating information regarding the nature of the information to be made available through the ISE. These notice mechanisms will also ensure that ISE recipients handle PI disseminated from mixed systems in accordance with applicable legal and DOT policy requirements. Notice will, to the extent feasible, permit ISE participants to determine whether the information pertains to a U.S. citizen or lawful permanent resident, is subject to specific information privacy or civil rights or civil liberties requirements, and has any limitations on reliability or accuracy.

Acceptable Use

38.4.4 PI collected by DOT may be used only for those purposes stated in the notice given to the individual or authorized by law, including a system of records notice (SORN). Prior

³ The Paperwork Reduction Act (PRA), 44 USC §§ 3501-3520, establishes a process for the review and approval of information collections from the public.

to using a record, system owners, with the assistance of their Departmental element Privacy Officer, must verify that:

38.4.4.1 The intended activity is listed as a routine use in the applicable SORN published in the Federal Register (if a Privacy Act system of records). If a routine use needs to be changed or added, modifications must be published in the Federal Register 30 days prior to those changes going into effect, and allow for interested persons to submit comments.

38.4.4.2 If the use is part of a computer matching program, that program meets all requirements listed in the computer matching provisions of the Privacy Act.

38.4.4.3 The individual consented to the use of the record for that purpose if the use is for a purpose other than that for which the record was collected, unless the use is otherwise authorized by law.

38.4.4.4 PI available from and shared by DOT in the ISE is used only in a manner that is consistent with the authorized purpose of the ISE.

Data Quality and Integrity

38.4.5 DOT uses and shares PI through the ISE only if it is considered reasonably accurate and appropriate for a documented purpose or to protect the integrity of the data.

38.4.6 DOT takes a number of steps to ensure data quality and integrity:

38.4.6.1 DOT investigates in a timely manner alleged errors and deficiencies in the information it shares in the ISE and corrects, deletes, or refrains from using PI found to be erroneous or deficient.

38.4.6.2 Upon receiving PI from an ISE participant that DOT determines may be inaccurate, DOT notifies in writing the appropriate authority within the contributing agency. As outlined in this Policy, prior to making any PI available within the ISE, notice is provided to the ISE participants that permits them to determine the nature of the information, including any limitations on the quality of the data.

38.4.6.3 Should DOT determine that PI is inaccurate or has been erroneously shared, it takes appropriate steps to provide in a timely manner written notice to the ISE participants that received the information and to request the correction or deletion of the inaccurate or erroneously shared information. The mechanism for such notice should be set forth in an information sharing agreement. In any event, written notice of the error and request for correction or deletion will be provided to ISE participants that received the inaccurate or erroneously shared information at issue through use of cover memoranda.

38.4.6.4 DOT also has redress mechanisms in place whereby, subject to applicable and appropriate exemptions claimed for DOT systems of records under the Privacy Act, individuals may request correction of their data. For more information, please refer to the section on Redress.

38.4.6.5 When merging PI about an individual (including partial matches) from two or more sources, DOT takes measures to ensure that the information is about the same individual.

38.4.6.6 DOT retains PI only so long as it is relevant and timely for appropriate use by DOT, and updates, deletes, or refrains from using PI that is outdated or otherwise irrelevant for such use.

38.4.6.6.1 Within the ISE, PI will be subject to the retention period defined by the DOT's privacy and records management compliance documentation including applicable System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), and authorized Records Disposition Schedules (RDS) covering the initial collection unless the information sharing agreements expressly modifies the retention period. For this reason, DOT Operating Administrations and Secretarial Offices should participate in the information sharing agreement process to ensure its data retention requirements are carried forward.

38.4.7 DOT also complies with the Information Dissemination Quality Guidelines drafted and adopted by DOT in response to OMB guidelines and the Treasury and General Government Appropriations Act for Fiscal Year 2001, Pub. L. No. 106-554. These guidelines provide measures for ensuring the quality and integrity of information maintained and disseminated by DOT and have been implemented by all DOT elements.

Sharing and Dissemination

38.4.8 DOT ensures that the PI that it makes available through the ISE has been lawfully obtained by DOT and may be lawfully shared and disseminated through the ISE. DOT will:

38.4.8.1 Share PI in the ISE only if it is terrorism-related information.

38.4.8.2 Review PI to be shared through the ISE before it is made available to the ISE.

38.4.8.3 Put in place a mechanism to enable DOT employees and the ISE participants with which it shares PI to determine the nature of the information, so it can be handled in accordance with applicable legal requirements.

38.4.8.4 Disseminate DOT employee personal information in accordance with appropriate privacy protections as required by law (e.g., the Privacy Act). DOT Human Resources is responsible for defining policies and procedures for protecting employee data and communicating those policies to all personnel who come in contact with the PI of DOT employees.

Access and Correction

38.4.9 In order to ensure the accuracy of PI used by DOT, individuals who submit information are afforded access to their records and have the ability to contest information they believe to be incorrect or incomplete about themselves. Individuals seeking access to any record containing information that is part of a DOT system of records, or seeking to contest the

accuracy of its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request to DOT.

38.4.9.1 Each Departmental element Privacy Officer is responsible for defining, documenting, and implementing policies for access to and correction of all classes of PI consistent with DOT policy.

38.4.9.2 Procedures have been developed at the Departmental level that document the process for receiving and responding to requests for access and correction of records.

Redress

38.4.10 If an individual has complaints or objections to the accuracy or completeness of PI allegedly acquired, accessed, stored, or shared by DOT through the ISE that has resulted in specific, demonstrable harm to such individual, and to which the individual has no right of access, DOT will inform the individual of the procedure for submitting and resolving complaints or requests for corrections.

38.4.11 Complaints and requests for corrections must be submitted to the DOT Chief Privacy Officer or designated representative per the procedures contained in DOT's regulations at 49 CFR Part 10. The DOT Chief Privacy Officer may be contacted at the following address: Privacy@dot.gov or Department of Transportation Headquarters, 1200 New Jersey Avenue, SE, Washington, DC 20590.

38.4.12 The Chief Privacy Officer acknowledges the complaint and states that it will be reviewed. The Chief Privacy Officer, however, is not required to confirm the existence or nonexistence of any information that is exempt from disclosure.

38.4.13 If the information complained of is held by DOT and may be shared in the ISE, but did not originate with DOT, the Chief Privacy Officer will notify the originating agency within 10 Federal work days in writing and will assist the originating agency upon request in correcting any identified data/record deficiencies, updating or purging the information, or verifying that the record is accurate. Any protected information originating with DOT is reviewed within 30 days and corrected in, updated, or purged from DOT data/records if it is determined to be erroneous, to include incorrectly merged information, or to be out of date. A record is kept by DOT of all complaints or requests for corrections and the action in response to the complaint.

Security

38.4.14 DOT provides adequate and effective security protection for PI shared through the ISE, in records stored and accessed in DOT systems to ensure their protection from unauthorized access, use, modification, or destruction. Each DOT element has developed policies and procedures to implement the following protections for systems that store PI that may be shared in the ISE:

38.4.14.1 Administrative, technical, and physical safeguards are in place to protect the security and confidentiality of PI.

38.4.14.2 All protections for PI and other sensitive information comply with the E-Government Act of 2002 (E-Gov); Federal Information Security Management Act of 2002 (FISMA); OMB Circular A-130, Appendix III; applicable National Institute of Science and Technology (NIST) security guidance; and Departmental security policies and procedures.

38.4.14.3 Records are securely retained and timely destroyed.

38.4.14.4 Security protection is commensurate with the risk level and magnitude of harm DOT and/or the record subject would face in the event of a data security breach.

38.4.14.5 ISE recipients of DOT PI demonstrate compliance with FISMA.

38.4.14.6 DOT has conducted privacy risk assessments and implemented administrative, technical, and physical mitigation strategies commensurate with the defined risk. DOT actively monitors and improves its privacy risk control measures as appropriate.

38.4.14.7 Additional information security requirements are defined in agency-to-agency or other information sharing access agreements.

Accountability, Enforcement, and Audit

38.4.15 In order to ensure the accountability and protection of PI shared in the ISE, DOT employs the following enforcement and audit procedures:

38.4.15.1 DOT requires that all of its personnel report, and appropriate personnel investigate and respond to, violations of agency policies relating to PI, including taking appropriate action when violations are discovered.

38.4.15.2 DOT requires that all of its personnel cooperate with audits and reviews by officials having responsibility for providing oversight with respect to the ISE.

38.4.15.3 DOT designated its Chief Privacy Officer as its ISE Privacy Official to receive reports (or copies, as appropriate) regarding alleged errors in PI that originate from DOT.

38.4.15.4 DOT established review and audit mechanisms to enable appropriate officials to verify that DOT and its personnel are complying with the ISE Privacy Guidelines.

Training

38.4.16 DOT's Chief Privacy Officer provides training to DOT personnel (i.e., employees, detailees, assignees, and contractors) and others authorized to share ISE information regarding DOT requirements and policies for collection, use, and disclosure of protected information and, as appropriate, for reporting violations of agency privacy protection policies. Awareness is the primary goal of the DOT privacy training program. Each DOT element is responsible for implementing such a program.

38.4.16.1 The following authorities require DOT personnel training:

38.4.16.1.1 Subsection (e)(9) of the Privacy Act of 1974, as amended, requires employee

training on the requirements of the Privacy Act.

38.4.16.1.2 OMB Memorandum M-01-05 *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy* iterates training required by the Privacy Act and emphasizes the need to communicate accountability and penalties under the law.

38.4.16.1.3 OMB Memorandum M-05-08 *Designation of Senior Agency Officials for Privacy* requires training for employees and contractors regarding information privacy laws, policies, and procedures governing each agency's handling of PI.

38.4.16.1.4 Section 522(a)(8) of Public Law 108-447, Consolidated Appropriation Act, 2005, requires training and educating employees on privacy and data protection policies to promote awareness and compliance.

38.4.16.2 Departmental guidance and content have been developed for use by each DOT element Privacy Officer in implementing annual training; however, DOT elements may develop their own training programs, provided they are consistent with legal requirements and DOT policy.

38.4.16.3 Training includes, at a minimum, the following:

38.4.16.3.1 Appropriate use and sharing of records covered by the Privacy Act;

38.4.16.3.2 Criminal and civil penalties for violating the Privacy Act;

38.4.16.3.3 Accountability for non-compliance with DOT policies;

38.4.16.3.4 Departmental policies and procedures; and

38.4.16.3.5 Any DOT element policies and procedures, as they relate to PI that may be shared in the ISE.

38.4.16.4 Training is provided to all personnel that have or may have access to PI that may be or has been shared in the ISE, or develop, manage, or maintain information systems that process and store PI that may be or has been shared in the ISE.

Awareness

38.4.17 DOT facilitates appropriate public awareness of its policies and procedures for implementing the ISE Privacy Guidelines and makes this Policy publicly available on request and on its Web site.

Required Procedures

38.4.18 DOT has developed Departmental procedures, located on the DOT intranet, to comply with requirements established in the Privacy Act of 1974. DOT elements may customize the Departmental procedures or develop their own, as needed, to meet their needs, provided they are consistent with all applicable legal requirements and DOT policy.

38.4.19 The following procedures are required by the Privacy Act of 1974:

38.4.19.1.1 Procedures to respond to individual requests to access records;

38.4.19.1.2 Procedures for disclosing records, including special procedures for sensitive records;

38.4.19.1.3 Procedures for reviewing and responding to requests to make changes to a record, including how to determine approval;

38.4.19.1.4 Procedures for monitoring recipient agencies in computer matching agreements for adequate security safeguards to protect PI; and

38.4.19.1.5 Procedures for the timely destruction of records received from other agencies as part of a computer matching agreement.

38.4.20 The Consolidated Appropriations Act, 2005, Pub. L. 108-447, includes the requirement of “training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies[.]”

Assessment of Policies and Update of Privacy Policy

38.4.21 DOT continuously seeks to identify and assess evolving laws, Executive Orders, policies, and procedures applicable to PI that DOT makes available or accesses through the ISE, and comply with any legal restrictions applicable to such information. This may require updating this policy as necessary to respond to evolving laws, Executive Orders, policies, and procedures.

(Table of Contents)

Section 38.5 Roles and Responsibilities

38.5.1 DOT Personnel engaged in the ISE are responsible for:

38.5.1.1 Complying fully with the Privacy Act of 1974 and other data protection laws referenced in this Policy.

38.5.1.2 Reviewing and signing a copy of this Policy to acknowledge that they received, reviewed, and understand its contents.

38.5.1.3 Contacting their DOT element Privacy Officer prior to beginning new collections or uses of PI to determine if a SORN and/or PIA needs to be written.

38.5.1.4 Providing adequate security protection and confidentiality for PI in their custody and use regardless of medium.

38.5.1.5 Attending Privacy Act and ISE Privacy and Civil Liberties training provided by their DOT element and completing any tests or attendance verification requested as part of the training.

38.5.2 Each system owner, in consultation with the appropriate Departmental element Privacy Officer, is responsible for identifying data holdings that contain PI. Once identified,

system owners are further responsible for ensuring that information is made available to the ISE in accordance with this Policy.

[\(Table of Contents\)](#)

Section 38.6 Dates

38.6.1 This DOT ISE Privacy Policy is effective as of the date signed.

[\(Table of Contents\)](#)

Section 38.7 Cancellations

38.7.1 None.

[\(Table of Contents\)](#)

Section 38.8 Compliance

38.8.1 This Policy, along with the Departmental ISE Policy, applies to all DOT offices, modes, and administrations.

38.8.2 DOT offices, modes, and administrations must comply with and support the implementation of the DOT ISE Policy, to include compliance with Federal requirements and programmatic policies, standards, and procedures for ISE operation. Non-compliance with the DOT ISE Privacy Policy, including failure to resolve or report violations of the Policy in a timely manner, must be reported to the appropriate DOT office, mode, or administration official for referral to DOT senior management for resolution.

[\(Table of Contents\)](#)

Section 38.9 Waivers

38.9.1 Compliance with this Policy is mandatory.

[\(Table of Contents\)](#)

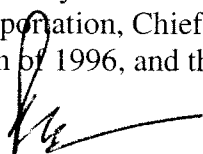
Section 38.10 Audit Procedures

38.10.1 This Policy will be reviewed on an annual basis alongside of the review of the Department's ISE Program.

[\(Table of Contents\)](#)

Section 38.11 Approval

This Policy has been approved and issued under the authority granted to the Secretary of Transportation, Chief Information Officer, in accordance with Public Law 104-106, Clinger-Cohen of 1996, and the Federal Information Security Management Act (FISMA) of 2002.



Nitin Pradhan
DOT Chief Information Officer

6/5/2012

Date

(Table of Contents)

Appendix A Glossary

Chief Privacy Officer, as defined by OMB Memorandum 05-07, is the senior official who has been identified to OMB by each agency as having overall responsibility for information privacy issues. DOT designated its Departmental Chief Information Officer for this role.

Computer Matching Program is a computerized comparison of two or more automated systems of records, or a system of Federal records with non-Federal records, with the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of, services with respect to cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs, or two or more automated Federal personnel or payroll systems of records, or a system of Federal personnel or payroll records with non-Federal records.

Departmental Chief Information Officer (CIO) is the senior management official who, with the DOT General Counsel, is responsible for the DOT Privacy Policy and Program.

Departmental Privacy Officer is the individual in the Office of the Secretary, appointed by the CIO, who is responsible for overseeing the implementation and management of the DOT's privacy policy and program.

Departmental Elements are offices within the Office of the Secretary (OST), the Operating Administrations (OAs), and any comparable components of DOT.

Departmental Element Privacy Officer is the individual responsible for implementation and management of the DOT Privacy Policy and Program at the level of a DOT Operating Administration, including OST.

DOT Information Sharing Environment (ISE) Program Manager is the senior official who represents DOT on the Information Sharing and Access Interagency Policy Committee and who is responsible for the overall conduct of DOT's ISE Program.

Individual at DOT includes a natural person, living or dead, regardless of nationality.

Information Sharing Environment (ISE) is an approach to the sharing of information related to terrorism that is being implemented through a combination of policies, procedures, and technologies designed to facilitate the sharing of critical information by all relevant entities. The ISE serves the dual imperatives of enhanced information sharing to combat terrorism and protecting the information privacy and other legal rights of Americans in the course of increased information access and collaboration. The ISE is being developed by bringing together, aligning, and building upon existing information sharing policies and business processes and technologies (systems), and by promoting a culture of information sharing through greater collaboration. It is being developed pursuant to Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of

2007 (IRTPA) and Executive Order 13388, entitled "Further Strengthening the Sharing of Terrorism Information to Protect Americans."

Information System Owner is a Federal Government employee who is responsible for planning, directing, and managing resources for an operational information system.

Mixed System is a dataset with terrorism-related PI that also contains PII about individuals whose information is not PI; in other words, some DOT datasets contain PII about individuals who are dead or who may not be U.S. citizens or legal permanent residents.

Personally Identifiable Information (PII) is any information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means, including both physical descriptors and online contact information.

Personnel includes both DOT Federal and contract employees.

Privacy Impact Assessment (PIA) is a documentation process that identifies and assesses security and privacy risks and mitigation efforts when planning, developing, implementing, and operating information management systems and rulemakings.

Protected Information is information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. Protected information to be made available within the ISE includes only homeland security information, law enforcement information, and terrorism information, including weapons of mass destruction information; these terms are defined as follows:

- **Homeland Security Information**, as derived from the Homeland Security Act of 2002, Public Law 107-296, Section 892(f)(1) (codified at 6 USC § 482(f)(1)), is defined as any information possessed by a State, local, tribal, or Federal agency that:
 - o Relates to a threat of terrorist activity;
 - o Relates to the ability to prevent, interdict, or disrupt terrorist activity;
 - o Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
 - o Would improve the response to a terrorist act.
- **Law Enforcement Information** is defined as any information obtained by or of interest to a law enforcement agency or official that is both:
 - o Related to terrorism or the security of our homeland, and
 - o Relevant to a law enforcement mission, including but not limited to:
 - § Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counter terrorism investigation;

- § An assessment of, or response to, criminal threats and vulnerabilities;
 - § The existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct;
 - § The existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law;
 - § Identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and
 - § Victim/witness assistance.
- **Terrorism Information** is defined in Section 1016 of the Intelligent Reform and Terrorism Prevention Act of 2004 (codified at 6 USC § 485) as all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:
 - o The existence, organization, capabilities, plans, intentions, vulnerabilities, means of financial or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
 - o Threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
 - o Communications of or by such groups or individuals; or
 - o Groups of individuals reasonably believed to be assisting or associated with such groups or individuals.

The definition includes weapons of mass destruction information.

- **Weapons of Mass Destruction Information** is defined in Section 1016 of the Intelligent Reform and Terrorism Prevention Act of 2004 (codified at 6 USC § 485) as information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or terrorist organization against the United States, including information about the location of a stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or terrorist organization against the United States.

Record, as defined by the Privacy Act of 1974, is any item, collection, or grouping of information about an individual that is maintained by a Federal agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or

employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Routine Use is defined in the system of records notice as the additional activities, uses, and disclosures that may take place for the record. Routine uses must be compatible with the primary uses of the system.

System of Records is a group of manual or electronic records maintained by the Federal Government from which information is retrieved by the name of the individual or identifying number, symbol, or other particular assigned to the individual. The Privacy Act applies to systems of records.

(Table of Contents)

Appendix B Authorities

Provided below are the authorities and guidance which support the development and execution of the DOT ISE Privacy Policy.

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, *as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007*, 50 USC § 402 *et seq.*

The Privacy Act of 1974, 5 USC § 552a *et seq.*, *as amended by The Computer Matching and Privacy Protection Act of 1988*, Pub. L. No. 100-503

The E-Government Act of 2002, Pub. L. No. 107-347, 44 USC Ch. 36

Federal Information Security Management Act of 2002, 44 USC § 3541

Homeland Security Act of 2002, Pub. L. No. 107-296

Executive Order 13311, Homeland Security Information Sharing (July 29, 2003)

Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans (October 25, 2005)

OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*

OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*

OMB Memorandum M-01-05 *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*

Final Guidance on Interpreting the Provisions of Public Law 105-503, 54 Fed. Reg. 25818 (June 16, 1989)

OMB Circular A-130 Revised, Transmittal Memorandum #4, Management of Federal Information Resources

DOT Notice of Establishment of Two New General Routine Uses and Republication of All General Routine Uses, 75 Fed. Reg. 82132 (Dec. 29, 2010)

DOT Privacy Act Information *available at* www.dot.gov/privacy

DOT's Guide for FOIA or Privacy Act Requesters *available at* www.dot.gov/foiareferenceguide.html

Chief Information Officer Policy (CIOP), DOT Order 1351.37 Departmental Cybersecurity Policy

(Table of Contents)