CIOP CHAPTER 1351.18

Departmental Privacy Risk Management Policy

TABLE OF CONTENTS

Section 18.1. Purpose

This policy establishes the Department of Transportation (DOT) policy and assigns responsibilities for carrying out the privacy risk management requirements of the Privacy Act of 1974 (Privacy Act), the Paperwork Reduction Act (PRA), the E-Government Act of 2002 (EGov), the Federal Information Security Management Act (FISMA) and the Consolidated Appropriations Act of 2005, as well as general privacy risk management at DOT.

These requirements often overlap, and special attention must be paid to each before commencing any collection of information or engaging in activities that may create privacy risk(s) for individuals and the larger public. This policy establishes policies and responsibilities for managing privacy risk in creating, collecting, maintaining, using, storing, transmitting, protecting and destroying personally identifiable information (PII).

PII is personal or professional information that can be used to distinguish or trace an individual's identity, such as the individual's name, Social Security number (SSN), biometric records, etc., alone or when combined with other personal or identifying

information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[1]

Further Office of Management and Budget (OMB) guidance states that "the definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements. During the assessment it is important for agencies to recognize that non-PII can become PII whenever additional information is made publicly available. This applies to any medium and any source that, when combined with other available information, could be used to identify an individual."[2]

This policy also establishes policies and responsibilities for managing privacy risk in activities that do not include the collection of PII by DOT.

(Table of Contents)

Section 18.2. Background

Privacy

In its mission to ensure a safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life, DOT collects, accesses and uses significant amounts of data every day. The DOT is committed to protecting the safety of all data throughout the system development lifecycle, but is especially aware of the risks associated with the collection, use, storage and sharing of PII.

The DOT's regulatory activities may also raise privacy concerns for members of the public by requiring regulated parties to collect information on individuals or implement technologies that may impact individual privacy.

It is vitally important that DOT not only protect this information, but also ensure that individuals be able to appropriately control the collection, use and sharing of their own PII within DOT information systems.

This policy is DOT's framework for identifying, assessing and mitigating privacy risk for information stored in DOT information systems.

Privacy Risk Management Lifecycle

With increased data collection, technology acceleration and regulatory complexity comes increased privacy risk, which is why DOT focuses on incorporating proactive risk management into every stage of program and information system development.[3] Risk

[1] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007

[2] OMB Memorandum 10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010

[3] Privacy risk constitutes a broad spectrum of potential unwanted or unwarranted activities including, but not limited to, the possibility of intrusion into an individual's personal space, unauthorized or unnecessary information

management improves compliance with privacy objectives by raising awareness among employees and leadership regarding the standards for data safety. It institutes frameworks for training, compliance assessment and vulnerability repair. Risk management activities can take place in four stages:

Develop the Risk Management Profile

This policy establishes DOT-wide privacy risk management guidance aligned to the Department's Strategic Plan and Annual Performance Plan. Each DOT Component may implement more rigorous privacy risk management standards as necessary based on specific mission requirements and information system privacy requirements.

Maintain Risk Management Standards

Privacy risk management standards will be managed to ensure they are developed, verified, versioned, used and sustained over time with the perspectives of all stakeholders in mind. Changes include changes to artifacts (e.g. System of Records Notices [SORN], Privacy Threshold Analyses [PTA], System Disposal Assessments [SDA], Privacy Impact Assessments [PIA]) and other privacy documentation and standards. Each DOT Component will maintain privacy data and artifacts that are relevant, current, and valid, as well as track and document changes in order for data and artifacts to be trusted for use in planning and decision-making.

Use Risk Management Tools

The artifacts, privacy risk management standards, and data from privacy risk analyses will support DOT decision-making on policies, including proposed rulemakings, information collections and operational matters like IT investments. Each DOT Component will use the privacy risk management standards documented in the policy to evaluate various policy and operational proposals under review by the Department.

Measure Risk Management Effectiveness

The DOT Privacy Risk Management program, as well as resultant analyses and mitigation strategies, will be evaluated on a regular basis to ensure DOT programs and the processes and systems used to support them maintain currency with privacy statutes, guidance and policies; accurately reflect DOT practice; and engender trust.

Overall, the privacy risk management lifecycle supports DOT's mission by reducing the possibility of errors in behaviors, technologies, and other business activities that could lead to undesirable privacy outcomes, including but not limited to the loss of public support, unauthorized use or access to PII, and increased oversight.

(Table of Contents)

collection or analysis, inappropriate use of or loss of control over information, and loss of benefits and privileges due to erroneous or poor quality data.

Section 18.3. Scope and Applicability

This policy applies to all DOT Component personnel.[4] This policy refers to all DOT Operating Administrations and Secretarial Offices collectively as "DOT Components." [5]

While this policy applies to all DOT Component activities, not all DOT activities create privacy risk and, of those activities that create privacy risk, not all privacy risk will rise to a level that requires the full spectrum of privacy compliance procedures and documentation outlined in this policy. Thus, the DOT Chief Privacy Officer (CPO) may develop and issue supplemental guidance as necessary to implement this policy and assist personnel in conducting their responsibilities in privacy risk management. Each DOT Component may issue additional policies and guidance provided they are consistent with existing laws, regulations, and DOT policies and procedures.

(Table of Contents)

Section 18.4. Policy

DOT is fully committed to protecting the personal privacy of all individuals. Certain privacy protections are stated in law; however, DOT recognizes that compliance with the letter of the law is not enough. DOT has a responsibility to ensure that individuals are treated with fairness and respect. DOT has established a Privacy Program to ensure that in addition to compliance with the law, the Fair Information Practice Principles remain integral to every policy decision and are observed and followed by all DOT employees and contractors.

The Fair Information Practice Principles (FIPPs)

The Fair Information Practice Principles (FIPPs) are a widely accepted framework that is at the core of the Privacy Act and is mirrored in other statutes, Federal policy and guidance. The FIPPs cover common privacy concerns and provide a universal platform for identifying, assessing and mitigating privacy risk. The DOT Privacy Office, therefore, has adopted the FIPPs as its privacy policy framework and seeks to apply them to the full breadth and diversity of DOT programs and activities.

The FIPPs provide the foundation of all DOT privacy policy development and implementation. The FIPPs must be applied whenever a DOT program or activity collects information or raises privacy concerns involving the collection of PII. In addition,

[4] Throughout this document, the term "personnel" is used to refer to all paid and unpaid members of the DOT staff, to include contractors and subcontractors. When used in this document, the term "contractor" refers to the organization, its employees, and the five types of contractors defined by OMB: service providers; contractor support; Government Owned, Contractor Operated facilities (GOCO); laboratories and research centers; and management and operating contracts. For more details regarding contractors, see OMB Memorandum M-14-04.

[5] All recommendations and requirements contained in this policy are applicable to all Components but only to the extent that such requirements and recommendations are consistent with the expressed language contained in 49 U.S.C 106, 40110, 40121. The Office of Inspector General (OIG) is not a Component as defined in this policy, but will issue internal policies consistent with this policy and work with the DOT Chief Privacy Officer when consistent with OIG independence.

the FIPPs will be applied to the deployment of any technology or development of any proposed or final regulation that raises privacy risks for individuals. This is a media-neutral policy and applies to all records regardless of whether they are created and/or maintained on paper or in an electronic format, unless otherwise specified in the policy.

To the extent practical and permitted by law, DOT extends its application of the FIPPs to all individuals living or deceased and to all individuals regardless of legal status.[6]

18.4.1. Transparency

The Department builds public trust and acceptance through public notice of its information practices and the privacy impact of its programs and activities. The Department also gives individuals the opportunity to comment on those practices and PIAs.

18.4.1.1. DOT will be transparent and provide notice to the individual regarding its collection, use, dissemination and maintenance of PII.

18.4.1.2. DOT will maintain no system of records without first giving public notice through a SORN published in the Federal Register.

18.4.1.2.1. DOT will publish a Privacy Act Exemption Rule (Exemption Rule) for any system of records the Department intends to exempt from portions of the Privacy Act.

18.4.1.3. DOT will, to the extent practical, make publically available its analysis of the privacy risks created by its information systems, programs or activities implemented through its regulations, information collections and any implemented risk mitigation strategies. At a minimum, and to the extent permitted by law, the DOT will make publically available approved PIAs, SORNs, Exemption Rules, and reports developed or created in response to oversight bodies including the OMB, Office of Inspector General (OIG), U.S. Congress and the Government Accountability Office (GAO).

18.4.1.3.1. DOT will, to the extent practical, make publically available its privacy practices, including but not limited to PIAs, SORNs and privacy reports.

18.4.1.4. DOT will provide means for the public to comment on privacy risk created by the Department and subsequent mitigation strategies.

[6] The Privacy Act of 1974 provides statutory privacy rights to U.S. citizens and Legal Permanent Residents (LPRs), (U.S. persons). The Privacy Act does not cover deceased individuals, visitors or aliens. OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, expressly authorizes agency extension of FIPPs coverage to non-U.S. citizen information. Any collection of PII containing information of both living U.S. persons and deceased individuals or U.S. persons and non-U.S. persons will be considered a "mixed system." As a matter of DOT policy, any PII collected, used, maintained and/or disseminated in connection with a "mixed system" by DOT will be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, alien or deceased individual. Non-U.S. persons have the right of access to their PII and the right to amend their records, absent an exemption under the Privacy Act; however, this policy does not extend or create a right of judicial review for deceased or non-U.S. persons.

18.4.1.5. DOT will provide a single consolidated online privacy policy explaining the Department's privacy-related practices pertaining to its official external website and its other online activities.

18.4.2. Individual Participation and Redress

By making individuals active participants in the decision-making process regarding the collection of their PII and providing opportunities to access, correct or amend PII, as appropriate, the Department enhances public confidence in PII-based decisions.

18.4.2.1. DOT will, to the extent practical, seek individual consent for the collection, use, dissemination and maintenance of PII.

18.4.2.1.1. When collection may result in adverse determinations about rights, benefits and privileges, DOT will make reasonable efforts to collect information directly from an individual.

18.4.2.1.2. DOT will receive consent from the individual for any new uses of previously collected PII.

18.4.2.2. DOT will provide mechanisms for appropriate access, correction and redress regarding DOT's use of PII.

18.4.2.3. DOT will implement a process for receiving and responding to complaints, concerns, or questions from individuals about organizational privacy practices.

18.4.3. Authority and Purpose Specification

The Department's programs and information systems are restricted in the collection and use of PII, or activity impacting privacy, to that which is authorized by law.

18.4.3.1. DOT will determine the legal authority that permits its collection, use, maintenance and sharing of PII, either generally or in support of a specific program or information system need.

18.4.3.2. DOT will clearly specify usage purposes within legal authorities.

18.4.3.3. DOT will maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained, or unless pertinent to and within the scope of an authorized law enforcement activity.

Internal Sharing

18.4.3.4. Unless otherwise limited by statute, information collected by a DOT Component will be considered an information asset of the entire Department.[7]

18.4.3.4.1. Unless explicitly authorized or mandated by law, DOT will permit internal sharing of PII only for a purpose compatible with the original purpose of collection, specified at the time of initial collection.

[7]This provision should not be construed as a basis for limiting or denying the Office of Inspector General access to PII that they are otherwise authorized to obtain.

18.4.3.4.2. DOT will document all authorized internal sharing of PII via a Memorandum of Understanding (MOU) or other approved instrument that articulates the conditions of access and use.

18.4.4. Data Minimization and Retention

The Department seeks to reduce its privacy and security risks by proactively limiting collected PII to that necessary for the proper performance of authorized business purposes. Regular efforts to ensure that PII holdings are accurate, relevant, timely and complete further reduce risk to the Department and individuals. DOT retains PII only so long as it is relevant and timely for appropriate use by DOT, and updates, deletes, or refrains from using PII that is outdated or otherwise irrelevant for such use.

18.4.4.1. DOT will collect only such information about an individual that is relevant and necessary for the proper performance of agency functions or to accomplish a purpose of the agency required by statute, regulation or executive order of the President.

18.4.4.2. DOT will minimize the use of PII for tests, training and research, and ensure that any such use of PII is compatible with the original purpose for which it was collected.

18.4.4.3. DOT will periodically review its PII holdings to determine if continued collection is necessary and appropriate and will eliminate any unnecessary holdings.

Social Security Numbers (SSNs)[8]

18.4.4.4. DOT will not collect or use SSNs as personal identifiers in connection with any information system or database, unless the collection and/or use is authorized and provided for by law.

18.4.4.4.1. DOT will review its SSN holdings on a regular periodic basis to ensure that such collection/retention/use continues to be both authorized and necessary.

18.4.4.4.2. DOT will remove any unauthorized or unnecessary collection, retention or use of SSNs.

18.4.4.5. DOT will make reasonable attempts to substitute other identifying information in place of collecting SSNs.

18.4.4.6. When requesting SSNs, DOT will inform individuals whether providing the SSN is mandatory or voluntary, any statutory or regulatory authority that authorized the collection of the SSN, and how the SSN collected will be used.

[8] Unless explicitly asserted to the contrary by the individual, an Employer Identification Number (EIN) provided by a sole proprietor will be considered a SSN and protected accordingly. Additional information about EIN may be found on the Internal Revenue Service website at http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Apply-for-an-Employer-Identification-Number-(EIN)-Online. Similarly, when DOT legacy systems permit the use of SSN in place of an alternative nine-digit identifier, such as Federal Aviation Administration (FAA) airman certification numbers, DOT will protect them accordingly.

18.4.4.7. DOT will not deny an individual any right, benefit, or privilege as a result of refusing to provide their SSN, unless the collection is authorized either by a statute or by a regulation issued prior to 1975.[9]

Retention

18.4.4.8. DOT will only retain PII for as long as necessary to fulfill the specified purpose(s) of collection.

18.4.4.9. DOT will ensure that PII is disposed of, destroyed and/or erased, regardless of the storage method, in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule and in a manner that prevents loss, theft, misuse or unauthorized access.

18.4.5. Use Limitation

The Department has committed to only use PII as specified in its public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Use limitation policy will ensure that the scope of PII use is restricted to these areas.

External Sharing

18.4.5.1. DOT will not sell or lease an individual's name and address unless such action is necessary and specifically authorized by law.

18.4.5.2. DOT will permit external sharing of PII only for a purpose compatible with the original purpose specified at the time of collection or that is authorized or mandated by law.

18.4.5.3. DOT will document all authorized external sharing of PII via an MOU or other approved instrument that explicitly defines the purpose, conditions and authorized use of shared information in connection with an authorized law enforcement activity under Section 552a(b)(7)) of the Privacy Act.

18.4.5.4. Prior to sharing any Privacy Act data, DOT will ensure that the recipient organization affords the appropriate equivalent level of management, operational and technical security controls as maintained by DOT.

Computer Matching Programs

18.4.5.5. All computer matching programs, as defined by the Privacy Act, between DOT and Federal, state or local governmental agencies will be conducted in accordance with applicable laws, regulations and policies.

18.4.5.6. DOT will not share any information via a computer matching program without first establishing a Computer Matching Agreement and publishing notice of the proposed match in the Federal Register.

[9] The Privacy Act of 1974, as amended, 5 U.S.C. 552a

18.4.5.7. DOT will establish a Data Integrity Board to oversee DOT Computer Matching Agreements and to ensure such agreements comply with the computer matching provisions of the Privacy Act.

18.4.6. Data Quality and Integrity

Information shall be sufficiently accurate, complete and up to date to minimize the possibility that inappropriate information may be used to make a decision about an individual. Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up to date, unless limits to the requirement for accuracy are clearly set out or exempted by law.

18.4.6.1. DOT will make reasonable efforts, prior to disseminating a record about an individual, to ensure that the record is accurate, relevant, timely and complete.

18.4.6.2. DOT will, to the extent feasible, establish mechanisms to allow individuals to access and correct information about themselves.

18.4.6.3. DOT will develop and implement reasonable procedures to ensure the accuracy of the data shared and the data received.

18.4.6.3.1. DOT will investigate alleged errors or deficiencies in PII that has been shared in a timely manner and will correct, delete or not use the PII if found to be inaccurate.

18.4.6.3.2. If DOT determines that PII is inaccurate, DOT will take timely, appropriate steps to provide written notice to the recipient of the shared data regarding the error and request that the inaccurate PII be corrected or deleted.

18.4.7. Security

Security standards ensure that technical, physical and administrative safeguards are in place to protect PII collected or maintained by the Department regardless of format or media.

18.4.7.1 DOT will protect PII through appropriate security safeguards against risks such as loss; unauthorized access, use, destruction or modification; or unintended or inappropriate disclosure.

18.4.7.1.1. DOT will protect all records against reasonably anticipated threats or hazards that could result in harm, embarrassment, inconvenience or unfairness to any individual about whom information is maintained.

18.4.7.1.2. At a minimum, all PII will be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentially standards.

18.4.7.1.2.1 The DOT CPO may, in accordance with OMB Memorandum 07-16 and FIPS 199, increase or decrease the accepted confidentiality risk of PII in a particular information system on a case-by-case basis, based on a determination about the risk of reasonably anticipated threats

or hazards that could result in harm to the individual or the Department as a result of unauthorized access or use of the PII.[10]

18.4.7.1.2.2 The confidentiality protection requirements of Sensitive PII (SPII) may not be reduced.[11]

18.4.7.2. DOT will implement encryption protections, using only National Institute of Standards and Technology (NIST)-certified cryptographic modules, for all electronic SPII being transported and/or stored offsite unless otherwise authorized, in writing, by the DOT Deputy Secretary or a Senior DOT Official.

18.4.7.3. PII will only be stored on federally owned or approved computers or mobile computing devices.

18.4.7.3.1. DOT will require all personnel requesting to maintain SPII on mobile computing devices or who work off site at any time to obtain documented authorization and conditions for any removal of Sensitive PII from DOT premises prior to any activity.

18.4.7.3.2. DOT will require all personnel who maintain SPII on mobile computing devices or who work off site at any time to ensure information is properly safeguarded against loss or compromise.

18.4.7.4. DOT will not print records containing PII unless required to support the DOT mission.

Incident Response

18.4.7.5. DOT will develop and implement a Privacy Incident Response Plan that provides an organized and effective response to privacy incidents.

18.4.7.5.1. DOT will ensure that all personnel are provided with a clear definition of what constitutes a breach involving PII and are aware of how, where and what information is needed to report the loss, inappropriate access, use or sharing of PII.

18.4.7.5.2. In the event of unauthorized PII access, use or disclosure, DOT will take immediate action to prohibit further damage or disclosure.

18.4.7.5.3. DOT will ensure appropriate and prompt notification of affected individuals in the event of a breach of SPII proportionate with the risk of harm to the individual(s) and consistent with Federal and DOT standards and requirements.

---

[10] OMB Memorandum 07-16 requires that agencies assign an impact level to all information and information systems, including minimum security requirements and controls. The following PII is not sensitive alone or in combination unless documented with sensitive qualifying information and may be treated as low confidentiality: name; professional or personal contact information including email, physical address, phone number and fax number.

[11] All Sensitive PII is de facto PII. As such, all references to PII should be read to include Sensitive PII. See Appendix A for a detailed discussion of PII and Sensitive PII.

18.4.8. Accountability and Auditing

Effective governance, monitoring, risk management and assessment controls demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

18.4.8.1. DOT will establish a Departmental Privacy Program, managed by the Departmental CPO, accountable for complying with this policy and auditing the actual use of PII to demonstrate compliance with the FIPPs and all applicable privacy protection requirements.

18.4.8.2. DOT will develop, disseminate and implement operational privacy policies and procedures that govern the appropriate privacy controls for programs, information systems or technologies.

18.4.8.2.1. DOT Components will establish appropriate privacy risk management programs to implement the Department Privacy Program.

18.4.8.3. DOT will establish internal and external reporting requirements or standards to ensure full accountability.

Training

18.4.8.4. DOT will require annual Privacy Act training for all DOT personnel.

18.4.8.4.1. Agency personnel (e.g. Component Privacy Officers, program officials, information systems personnel, personnel specialists, finance officers, investigators, acquisition officials, attorneys/advisors, public affairs and disclosure officials) who maintain or have access to PII, regardless of medium, will receive specialized privacy training before being granted access to that information and/or system.

18.4.8.4.2. DOT will ensure that all personnel, including contractors, involved in the design, development, operation, maintenance or control of any system of records are informed of all requirements to protect the privacy of the individuals whose information is contained in the records and sign a Privacy Rules of Behavior Acknowledgement.

Contracts

18.4.8.5. DOT will include appropriate privacy requirements in all contracts and other acquisition-related documents for DOT systems developed, maintained, operated, and or managed by contractors that contain PII.

18.4.8.6. DOT will ensure all contractors maintaining information systems containing PII will have contracts that contain the appropriate clauses as may be required by Federal Acquisition Regulations (FAR) and other Federal authorities in order to ensure that the PII under the control of the contractor is maintained in accordance with Federal law and DOT policy.

18.4.8.6.1. DOT will obtain contractual assurances from third parties working on official DOT business that the third parties will protect PII in a manner consistent

with the privacy practices of the Department during all phases of the system development lifecycle.

(Table of Contents)

Section 18.5. Roles and Responsibilities

This section defines the roles key to implementing the Departmental Privacy Program and privacy-specific responsibilities associated with each role. Provided below is a summary listing of the roles and the levels in the organization where they reside. The Departmental Chief Privacy Officer is designated the primary operational officer.

Department Level

- Department Chief Information Officer
- Department Chief Privacy Officer
- Department Chief Information Security Officer
- Office of General Counsel
- Senior Procurement Executive

Component Level

- Component Chief Information Officer
- Component Privacy Officer
- Component Information Systems Security Manager
- Component Office of Chief Counsel

Program Level

- Business Owners
- Contracting Officer
- System Owners

DOT-Wide

- All DOT Employees and Contractors

Department Level

18.5.1. Accountability for directing DOT's information and data integrity, and for all IT functions, resides with the DOT Chief Information Officer (CIO). In addition to responsibilities listed elsewhere in Departmental policy, the **DOT CIO** serves as the Departmental Senior Agency Official for Privacy (SAOP), as required in OMB Memo M-05-08. **The DOT CIO** will:

18.5.1.1. Appoint a Departmental Chief Privacy Act Officer to assist with implementation, evaluation and administration issues of the Privacy Act.[12]

[12] 49 CFR 10.13

18.5.1.2. Ensure a Departmental Privacy Program is developed, documented and implemented to support privacy and risk management activities for all information systems, networks and data that support departmental operations.

18.5.1.3. Maintain a central policy-making role in the organization's development and evaluation of legislative, regulatory and related policy proposals involving privacy issues.

18.5.1.4. Ensure the organization establishes and implements information privacy protections, including full compliance with Federal laws, regulations and policies relating to privacy protection.

18.5.1.5. Ensure privacy risk management processes are integrated with DOT strategic and operational planning processes.

18.5.1.6. Provide resources to administer the Departmental Privacy Program.

18.5.1.7. Promote privacy policy compliance and risk management throughout the Department.

18.5.2. Operationalization of the Departmental Privacy Program is assigned to the Departmental Chief Privacy Officer. The **Departmental Chief Privacy Officer (DOT CPO)** will:

18.5.2.1. Serve as the Departmental Chief Privacy Act Officer.

18.5.2.2. Serve as lead privacy analyst for inter-agency initiatives with privacy impact.

18.5.2.3. Oversee the implementation of a robust privacy program that includes the adoption of policies, procedures and privacy documentation consistent with applicable laws and regulations.

18.5.2.4. Ensure the organization's implementation of information privacy protections, including the organization's full compliance with Federal laws, regulations and policies relating to privacy protection.

18.5.2.5. Exercise a central role in overseeing, coordinating and facilitating the organization's privacy compliance and risk management activities. This role includes establishing and periodically reviewing/updating the organization's privacy procedures to ensure that they are comprehensive and current.

18.5.2.6. Evaluate new technologies, programs, online activities, contracts, regulations and legislation for potential privacy impacts prior to commencing any activity, and advise other members of senior leadership on implementation of corresponding privacy protections.

18.5.2.7. Serve as the agency official in charge of developing and implementing an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

18.5.2.7.1. Approve or disapprove the closure of all DOT privacy-related incidents in accordance with the Privacy Incident Response Plan.

18.5.2.8. Engage in close collaboration with key organization officials, including the CIO, Chief Information Security Officer (CISO), business owners, privacy personnel and others, to discuss new initiatives and integration of regular privacy risk management throughout the System Development Life Cycle.

18.5.2.8.1. Ensure that Departmental risk posture is verified and maintained and that the privacy program’s mission is fully integrated into the organization's risk management practices.

18.5.2.9. Establish the framework for privacy- and risk management-related reporting activities, including initiating and updating SORNs, PTAs, PIAs, SDAs and other privacy risk management and compliance documentation.

18.5.2.9.1. Review and approve privacy-related risk management and compliance strategies and documentation, including PIAs, PTAs, SORNs and SDAs, prior to any required publication.

18.5.2.9.2. DOT CPO approval of privacy risk management strategy is required as a precondition for the issuance of an authorization to operate. The authority for selection and assessment of privacy controls ultimately rests with SAOP.

18.5.2.10. Approve the Department’s submission of privacy reporting activities, in coordination with input from Department and Component officials as applicable.

18.5.2.11. Develop a training program to ensure that employees and contractors receive appropriate training regarding the Privacy Act and associated orders, regulations and OMB guidance.

18.5.3. The **Departmental Chief Information Security Officer (DOT CISO)** will:

18.5.3.1. Require that component Information Systems Security Managers (ISSMs) or designees include methods to evaluate the privacy risk for new information systems or changes to existing information systems and implement necessary security controls to mitigate identified risk throughout the System Development Lifecycle.

18.5.3.2. Advise and support the DOT CPO in all security-related aspects of privacy risk management and breach response.

18.5.3.3. Alert the CIO, DOT CPO and all other relevant parties in the case of any security breach with risk to PII or privacy risk management implications.

18.5.4. The **DOT Office of the General Counsel (OGC)** will consult with the DOT CPO to:

18.5.4.1. Identify the laws, regulations and internal policies that apply to PII and provide guidance to the DOT CPO of the impact or implementation requirements of the same

18.5.4.2. Provide information to the DOT CPO to help identify DOT proposed regulations that may create privacy risk.

18.5.4.3. Interpret statutory language to ensure there is a close nexus between the general authorization and any specific collection of PII.

18.5.4.4. Participate in the drafting process for privacy notices, information collections and rulemakings.

18.5.5. The **Office of the Senior Procurement Executive (SPE)** will:

18.5.5.1. Partner with the DOT CIO to develop and implement IT privacy-related contract clauses for incorporation in all current and future contracts and covered grants.

18.5.5.2. Promote the appropriate use of the required clauses in all applicable contracts.

18.5.5.3. Ensure contracting officers (COs) enforce the requirements of IT privacy clauses.

Component Level

18.5.6. Accountability for directing the information and data integrity of the Component and its groups, and for all IT functions, resides with the Component Chief Information Officer. In addition to responsibilities listed elsewhere in Departmental policy, the **Component Chief Information Officer** will:

18.5.6.1. Coordinate with Component budgetary offices to ensure appropriate privacy risk management activities and documentation are included as part of capital asset planning and investment control (CPIC) processes.

18.5.6.2. Ensure the Component Privacy Office is appropriately staffed and resourced.

18.5.7. The Component Privacy Officer serves as the primary point of contact on Component privacy concerns and implementation of the Component privacy program.[13] The **Component Privacy Officer (PO)** will:

18.5.7.1. Serve as the primary official for assisting the Component in implementing the FIPPs and this policy.

18.5.7.2. Advise senior Component officials on proper procedural, contractual, technical, or programmatic actions to correct privacy-related deficiencies.

18.5.7.3. Implement the DOT system for privacy risk management assessment for rulemaking.

18.5.7.4. Conduct oversight of privacy risk management activities within the Component including, but not limited to, designing, coordinating, implementing and supporting risk management activities in accordance with guidance.

18.5.7.4.1. Work with the Component Information Systems Security Manager(s) (ISSM) or equivalent designee(s) to determine the confidentiality risk and associated mitigations of information systems.

18.5.7.4.2. Ensure any controls intended to mitigate privacy risk are implemented and effective.

18.5.7.5. Ensure appropriate privacy protections are developed, implemented and verified for PII that is collected, stored, disseminated, transmitted, or disposed of by information systems owned or operated by or for the Component.

18.5.7.6. Implement, consistent with guidance and processes established by the DOT CPO, the Component process for the completion, review, tracking and approval of privacy compliance and risk management strategies and documents including, but not limited to, PIAs, PTAs and SORNs.

18.5.7.6.1. Review completed Component PIAs, PTAs and SORNs to ensure they are adequate and accurate before submission to the DOT CPO for final approval.

18.5.7.7. Coordinate Component privacy compliance documentation to ensure that the Department management, technical and operational privacy requirements are addressed.

18.5.7.8. Ensure that Component websites, including those funded by the Component, comply with and include the approved DOT online privacy policy.

18.5.7.9. Ensure that all DOT personnel[14] are trained annually regarding the Privacy Act and associated orders, regulations and OMB guidance.

[13] DOT Components have broad flexibility in determining the appropriate reporting structure for their privacy programs based on the organization's privacy risk.

18.5.7.9.1. In the case that component officials determine there is a need for specialized role-based training, they will develop and issue said training as required.

18.5.8. The privacy-related responsibilities of **Component Information Systems Security Managers (ISSM)** or equivalent designees include, but are not limited to:

18.5.8.1. Working with the Component PO to evaluate the privacy risk of an information system and implement necessary security controls to mitigate identified risk.

18.5.8.1.1. Evaluating the sensitivity of any PII accessed, created, used or retained in the information system.

18.5.8.1.2. Consulting with the Component PO for reporting and handling privacy incidents.

18.5.9. The **Component Chief Counsel** will work with the Component PO and other Component and Departmental officials to:

18.5.9.1. Identify the laws, regulations and internal policies that apply to PII and provide guidance to the Component PO on the impact or implementation requirements of the same.

18.5.9.2. Provide information to the Component PO to help identify Component proposed regulations that may create privacy risk.

18.5.9.3. Interpret statutory language to ensure there is a sufficient nexus between the general authorization and any specific collection of PII.

18.5.9.4. Participate in the Component drafting process for privacy notices, information collections and rulemakings.

Program Level

18.5.10. A Business Owner is the champion of the service, activity, or information system and owner of the requirement for the service, activity or system. **Business Owners** will:

18.5.10.1. Ensure resources are appropriately requested and applied to identify, evaluate and mitigate privacy risk.

18.5.10.2. Communicate business requirements for the collection, use and retention of PII to the Component PO during the privacy risk assessment process and prior to the use or collection of PII.

18.5.10.3. Ensure business operations use information consistent with published SORN and exemption rules and notify Component PO of any proposed use not explicitly covered in those notices.

18.5.10.4. Notify the Component PO when establishing, revising or deleting an information system containing PII.

18.5.10.4.1. Notice must be sufficiently timely to allow the Component PO to conduct necessary privacy risk management analysis and determine appropriate mitigation strategy.

18.5.10.5. Manage the privacy risk management process among information system owners who collect, manage, use, share or delete PII to ensure evaluations are conducted in a timely and efficient manner.

18.5.10.5.1. Periodically review PII holdings to determine and recommend to the Component PO whether continued collection is necessary and appropriate.

18.5.10.6. Ensure risk mitigation strategies are implemented in a timely and effective manner and monitor to ensure information system protections are being applied or will be applied to ensure adequate protection of the data.

18.5.10.7. Begin the PIA process when a new information system is proposed that will collect, store, or process identifiable information; when starting to significantly modify an existing information system; or when a new electronic collection of identifiable information is being proposed.

18.5.10.7.1. Collaborate with the Component PO to draft a SORN for each new, significantly altered and terminated system of records throughout the lifecycle of the system.

18.5.10.7.2. Collaborate with System Owners to ensure all privacy regulatory compliance reporting is entered and updated as required in the Cyber Security Assessment and Management (CSAM) system and/or any other DOT tracking system.

18.5.11. The Contracting Officer has the authority to enter into, administer and/or terminate contracts, and make related determinations and findings. The **Contracting Officer** or **Contracting Officer's Representative** will;

18.5.11.1. Coordinate with the System Owners, Business Owners, Project Officers/Managers and Component PO to ensure that the appropriate privacy risk management language from the DOT Chief Procurement Officer and other relevant sources is incorporated into all contracts.

18.5.11.2. Work with the System Owners, Business Owners, Project Officers/Managers and DOT PO to ensure that contractual privacy risk management obligations are upheld.

18.5.11.3. Advise contractors that develop or maintain a Privacy Act System of Records on behalf of the Federal Government that the Privacy Act applies to them to the same extent that it applies to the government, per subsection (m) of the Privacy Act.

18.5.11.4. Coordinate with the Component PO regarding deliverable acceptance, and reject deliverables that create privacy risk or do not meet privacy obligations as defined in FAR and/or contracts.

18.5.11.4.1. The Contracting Officer will not accept final privacy risk management deliverables requiring DOT PO approval without said approval.

18.5.11.5. Determine the applicability of the Privacy Act with assistance from the DOT Component Privacy Office and Component Office of Chief Counsel when the design, development, or operation of a Privacy Act SOR on individuals is required to accomplish an agency function.

18.5.11.6. Report actual or suspected privacy-related incidents, including PII breaches and violations by contracted personnel or contracted parties, to the DOT CPO and Component PO in a manner consistent with DOT policy.

18.5.11.7. Ensure that any remediation directed at contracted personnel or contracted parties for PII breaches or violations is implemented as required.

18.5.12. The System Owner is the key point of contact (POC) for the information system and is responsible for coordinating System Development Life Cycle activities specific to the information system.[15] **System Owners** will:

18.5.12.1. Ensure the information system is operated according to applicable privacy controls.

18.5.12.2. Monitor and immediately report any suspected or confirmed breaches of Privacy Act Records, and other records containing PII, to the Component PO.

18.5.12.3. Ensure that all proper measures are taken to ensure confidentiality of PII on all information systems for which they are responsible.

DOT-Wide

18.5.13. All **DOT Component Personnel** will:

18.5.13.1. Report all suspected and actual unauthorized collection, use, maintenance, dissemination and deletion of PII.

18.5.13.2. Participate in training and awareness programs on privacy and data protection policies, information privacy laws, and Departmental regulations, policies and procedures to promote awareness of and compliance with established privacy and data protection policies.

18.5.13.3. Acknowledge PII responsibilities to ensure that PII is only used as authorized.

18.5.13.4. Adhere to the DOT Privacy and Security Rules of Conduct.

(Table of Contents)

[15] NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

Section 18.6. Dates

18.6.1 The effective date of this policy is the date the policy is approved.

18.6.2 The DOT will meet all reporting deadlines consistent with the most recent OMB privacy guidance.

18.6.3 In accordance with the CIOP and the DOT Order Directive Process, this chapter will be reviewed annually and validated by the DOT CPO. The policy content will be annually reviewed to ensure it has clear intent, contains the right material and complies with the IT Directive Publication Process. Roles and responsibilities will be reviewed and updated on a quarterly basis.

(Table of Contents)

Section 18.7. Cancellations

18.7.1 This policy supersedes the following previously issued policy and guidance:

- Order 1351.20, CIOP Chapter 20, U.S. Department of Transportation Rules of Conduct and Consequences Policy Relative to Safeguarding Personally Identifiable Information, signed by the Acting DOT CIO on June 30, 2009.
- DOT Information Technology and Information Assurance Policy Number 2006-22 (revision 1): Implementation of DOT's Protection of Sensitive Personally Identifiable Information (SPII), October 11, 2006
- DIRMM Chapter 8 - Privacy Protections, January 2006

(Table of Contents)

Section 18.8. Compliance

18.8.1 The DOT Components must comply with and support the implementation of a Departmental Privacy Program, to include compliance with Federal requirements and programmatic policies, standards, procedures and information system privacy controls. This policy applies to all DOT Components (and organizations conducting business for and on behalf of the Department through contractual relationships when using DOT IT resources). This policy does not supersede any other applicable law, higher-level agency policy, or existing labor management agreement in place as of the effective date of this policy.

18.8.2 Departmental officials must apply this Departmental Privacy Policy to employees, contractor personnel, interns and other non-government employees. All DOT Components collecting or maintaining information, or using or operating information systems on behalf of the Department, are also subject to this Departmental Privacy Policy. The content of this Departmental Privacy Policy must be incorporated into applicable contract language as appropriate.

18.8.3 Any person who improperly discloses PII is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act). DOT Components must

comply with this Policy in accordance with statements outlined in Section 18.3 Scope and Applicability of this policy.

18.8.4 Non-compliance with the Departmental Privacy Policy, including failure to resolve or report privacy breaches in a timely manner, must be reported to the appropriate DOT Component for referral to DOT senior management for resolution up to and including temporary or permanent discontinuation of the non-compliant system.

18.8.5 DOT personnel may be subject to the following consequences for non-compliance with this policy:

18.8.5.1 Any personnel that willfully maintains a Privacy Act system of records without meeting the publication requirements is subject to possible criminal or civil penalties, administrative sanctions, or any combination.

18.8.5.2 Any personnel with possession of, or access to, PII that willfully discloses that material in any manner to any person or agency not entitled to receive it may be guilty of a misdemeanor and fined not more than $5,000.[16]

18.8.5.3 Personnel may be subject to written reprimand, suspension, or removal under the following situations:

- Knowingly failing to implement and maintain information security controls required for the protection of PII and PII systems regardless of whether such action results in the loss of control or unauthorized disclosure of PII. The minimum consequence is prompt removal of authority to access information or systems from individuals who demonstrate egregious disregard or a pattern of error in safeguarding PII.
- Failing to report any known or suspected loss of control over or unauthorized disclosure of PII
- For managers, failing to adequately instruct, train, or supervise employees in their responsibilities.

(Table of Contents)

Section 18.9. Waivers

18.9.1 Compliance with this policy is mandatory.

18.9.2 The DOT Components may request that the DOT CPO grant a waiver of compliance based on a compelling business reason. In addition to an explanation of the waiver sought, the request must include: (1) justification, (2) what measures have been implemented to ensure that privacy principles have been implemented (3) waiver period and (4) milestones to achieve compliance. The DOT CPO will provide a written waiver or justification for denial.

(Table of Contents)

[16] The Privacy Act of 1974, as amended, 5 U.S.C. 552a

Section 18.10. Audit Procedures

18.10.1 In order to ensure the Department provides appropriate accountability for privacy, and that the DOT CPO provides active support and oversight of monitoring and improvement of the Departmental Privacy Program, the DOT CPO must:

18.10.1.1. Develop and implement an oversight and compliance function to provide the required guidance and reviews to meet the Privacy Act, E-Government Act, and other government-wide privacy requirements;

18.10.1.2. Conduct annual compliance reviews of DOT Component Privacy Programs;

18.10.1.3. Develop and manage Privacy Plans of Actions and Milestones (POA&M) for the Departmental Privacy Program reporting progress to the DOT CIO and Secretary of Transportation;

18.10.1.4. Monitor Component efforts to identify and address weaknesses in their respective Privacy Programs; and

18.10.1.5. Ensure that corrective actions identified as part of the assessment process are tracked and monitored until findings are corrected.

18.10.2 DOT will conduct an audit of its privacy program as required by Section 522 of the Consolidated Appropriations Act, as amended.

(Table of Contents)

Section 18.11. Approval

X SEP 30 2014

Richard McKinney
DOT Chief Information Officer

(Table of Contents)

Appendix A Definition of Terms

Breach. Includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other-than-authorized purpose have access or potential access to PII regardless of format.

Business Owner: The spokesperson for the IT service initiative and the owner of the business, functional and funding requirements for the system/service throughout the business's life cycle, from concept to disposal. The business owner works with various parties depending on the life cycle phase of the business. (Source: DOT OCIO IT Governance Guidance Memo, June 2010)

Computer Matching. Any computerized comparison of (A) two or more automated systems of records or a system of records with non-federal records for the purpose of-- (i) establishing or verifying the eligibility of (or continuing compliance with statutory and regulatory requirements by) applicants for cash or in-kind assistance or payments under federal benefit programs, or recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments or (ii) recouping payments or delinquent debts under such federal benefit programs or (B) two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. Computer Matching activities must be documented in a Computer Matching Agreement.

Identifiable Form. Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Individual. A citizen of the United States or an alien lawfully admitted to the United States whose name or other personal identifier is used to retrieve records from a system of records.

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: NIST SP 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems)

Mixed System. Any System of Records that collects, maintains, or disseminates information in an identifiable form, and which contains information about U.S. Persons (citizens and legal permanent residents) and non-U.S. Persons. Any System of Records that collects, maintains, or disseminates information in an identifiable form, and which contains information about U.S. Persons both living and deceased. DOT will apply the fair information practice principles in the development and maintenance of mixed systems.

Personally Identifiable Information (PII). PII is information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number,

biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Certain PII, while not sensitive PII, may be Sensitive Security Information (SSI) under 49 CFR Part 15 or 49 CFR Part 1520. PII that is SSI must be maintained, disseminated, and destroyed in accordance with this policy, the Privacy Act (if applicable), and the applicable SSI requirements at 49 CFR Part 15 or 1520.

Privacy Impact Assessment (PIA). An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Threshold Analysis (PTA). A survey of questions that is prepared for all new systems and any other investment that undergoes substantial modifications. The PTA determines if the investment will be collecting any PII data elements and if a full Privacy Impact Assessment is required.

Record. In the context of the Privacy Policy, any item, collection or grouping of information about an individual that is maintained by an agency, e.g., the individual's education, financial transactions and medical, criminal or employment history, and that contains the individual's name or any identifying number, symbol or particular assigned to the individual.

Risk-based Approach. An activity, mechanism, or methodology that is designed to provide "adequate security" (as defined in OMB Cir. A-130, Appendix III) for the affected IT and/or information resources. In the context of this policy, this applies principally to the security objective of confidentiality.

Routine Use. Any outside disclosure of Privacy Act information in which the use is compatible with the purpose for which the information was collected. Routine uses must be included in the published notice for the system of records involved.

Sensitive Personally Identifiable Information (Sensitive PII or SPII) is a subset of PII which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

The following PII is always *(de facto)* sensitive, with or without any associated personal information, and cannot be treated as low confidentiality:

- Social Security number (SSN)
- Passport number
- Driver's license number

- Vehicle Identification Number (VIN)
- Biometrics, such as finger or iris print, and DNA
- Financial account number such as credit card or bank account number
- The combination of any individual identifier and date of birth, or mother's maiden name, or last four of an individual's SSN

The following information is Sensitive PII when associated with an individual:

- Account passwords
- Criminal history
- Ethnic or religious affiliation
- Last 4 digits of SSN
- Mother's maiden name
- Medical Information
- Sexual orientation

In addition to *de facto* Sensitive PII, some PII may be deemed sensitive based on context. For example, a list of employee names is not Sensitive PII; however, a list of employees' names and their performance rating would be considered Sensitive PII.

The following PII is not sensitive alone or in combination unless documented with sensitive qualifying information and may be treated as low confidentiality:

- Name
- Professional or personal contact information including email, physical address, phone number and fax number

Federal employee name, work contact information, grade, salary and position are considered PII. Except for limited circumstances, this information is publically available and is not considered sensitive.

System Owner. The key POC for the system who is responsible for coordinating SDLC activities specific to the system. It is important that this person have expert knowledge of the system capabilities and functionality. (Source: NIST 800-18rev1)

System Development Lifecycle (SDLC). The method of protecting information and information systems by integrating security and privacy into every step of the system development process. The multistep process starts with initiation, analysis, design, and implementation, and continues through the maintenance and disposal of a system.

System Disposition Assessment (SDA). A survey of questions that is prepared for all systems and any other investment at the end of their life-cycle. The SDA determines actions necessary to ensure appropriate privacy risk management as the system/investment is retired or migrated.

System of Records (SOR). A group of records under the control of a DOT component, from which information is retrieved by the individual's name or some identifying number,

symbol, or other identifying particular assigned to the individual. Notices for all Privacy Act systems of records must be published in the Federal Register.

(Table of Contents)

Appendix B Legal Authorities and Guidance

Legislation

- The Privacy Act of 1974, as amended, 5 U.S.C. 552a
- The Paperwork Reduction Act of 1995, as amended, 44 U.S.C. 3501, et seq.
- E-Government Act of 2002, P.L. 107-347
- The Omnibus Spending Bill for Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005, section 522
- Clinger-Cohen Act of 1996, P.L. 104-106
- Confidential Information Protection and Statistical Efficiency Act, P.L. 107-347, Title V
- Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-06
- Computer Matching and Privacy Protection Act of 1988, P.L. 100-503
- Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et. seq.
- Freedom of Information Act of 1966, as amended, 5 U.S.C. 552
- Federal Information Security Management Act, P.L. 107-347, Title III
- Government Paperwork Elimination Act, P.L. 105-277, Title XVII

National Policy, Directives and Memoranda

- OMB Circular A-130, Transmittal Memorandum #4, "Management of Federal Information Resources"
- Office of Management and Budget (OMB) Privacy Act Implementation Guidelines and Responsibilities
- OMB PRA Implementation Guidance, 5 C.F.R. Part 1320
- Code of Federal Regulations, Title 49, Transportation, Subtitle A, Maintenance of And Access to Records Pertaining to Individuals, October 1, 2014
- OMB Memorandum M-83-11, Guidelines on the Relationship Between the Privacy Act of 1974 and the Debt Collection Act of 1982
- OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"
- OMB Memorandum M-99-18, Privacy Policies on Federal Websites
- OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites

- OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
- OMB Memorandum M-03-18, Implementation Guidance for the E-Government Act of 2002
- OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB Memorandum M-05-04, Policies for Federal Agency Public Websites
- OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy
- OMB Memorandum M-06-06, Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information
- OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information, Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M-07-16, Safeguarding Against and responding to the Breach of Personally Identifiable Information
- OMB Memorandum M-10-22, Guidance for the Online Use of Web Measurement and Customization Technologies
- OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications
- OMB Memorandum M-11-02, Sharing Data While Protecting Privacy
- OMB Memorandum M-11-29, Chief Information Officer Authorities
- OMB Memorandum M-13-13, Open Data Policy - Managing Information as an Asset
- OMB Memorandum M-13-20, Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative
- OMB Memorandum M-14-04, Fiscal year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.
- OMB Memorandum M-14-06, Guidance for Providing and Using Administrative Data for Statistical Purposes
- Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act o1 1974, 56 FR 18599
- Final Guidance Interpreting the Privacy Provisions of Public Law 100-503, the Computer Matching and Privacy Protections Act of 1988, 54 FR 25818

- Guidance on Privacy Act Implementations of Call Detail Programs, 54 FR 12290
- Implementation of the Privacy Act of 1974, Supplemental Guidance, 40 FR 5674,
- Congressional Inquiries which Entail Access to Personal Information Subject to the Privacy Act
- Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948
- Executive Order 13478, Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers
- Biennial Privacy Act and Computer Matching Reports (June 1998)
- Privacy Act Responsibilities for Implementing the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (November 3, 1997)

National Standards

- National Institute of Standards and Technology Special Publication (SP) 800-53 Revision 4– Privacy and Security Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology SP 800-144 – Guidelines on Security and Privacy in Public Cloud Computing
- National Institute of Standards and Technology SP 800-122 – Guide to Protecting the Confidentiality of PII
- NIST Special Publication 800-18 Revision 1 – Guide for Developing Security Plans for Federal Information Systems
- Federal Information Processing Standard 199, Standards for Security Categorization of Federal Information and Information Systems

DOT Policies

- U.S. Department of Transportation Information Technology Governance Policy (DOT Order 1351.39)
- U.S. Department of Transportation Privacy Policy for the Information Sharing Environment (DOT Order 1351.38)
- U.S. Department of Transportation Cybersecurity Policy (DOT Order 1351.37)
- U.S. Department of Transportation Data Release Policy (DOT Order 1351.34)
- U.S. Department of Transportation Paperwork Reduction Act and Information Collection Policy (DOT Order 1351.29)
- U.S. Department of Transportation Web Policy (DOT Order 1351.24)

- U.S. Department of Transportation Rules of Conduct and Consequences Policy Relative to Safeguarding Personally Identifiable Information (DOT Order 1351.20)
- U.S. Department of Transportation Personally Identifiable Information Breach Notification Controls (DOT Order 1351.19)
- U.S. Department of Transportation Records Management Policy (DOT Order 1351.28)

Guidance

- Agencies' Efforts to Implement OMB's *Privacy* Policy GGD-00-191, Sep 5, 2000
- Key Challenges Facing Federal Agencies GAO-06-777T, May 17, 2006
- Preventing and Responding to Improper Disclosures of Personal Information GAO-06-833T, Jun 8, 2006
- Lessons Learned about Data Breach Notification GAO-07-657, Apr 30, 2007
- Recommendations for Identity Theft Related Data Breach Notification, Sep 2006
- Government Use of Data from Information Resellers Could Include Better Protections GAO-08-543T, Mar 11, 2008
- Alternatives Exist for Enhancing Protection of Personally Identifiable Information GAO-08-536, May 19, 2008
- Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions GAO-08-603, May 30, 2008
- OPM Should Better Monitor Implementation of *Privacy*-Related Policies and Procedures for Background Investigations GAO-10-849, Sep 7, 2010
- Federal Law Should Be Updated to Address Changing Technology Landscape GAO-12-961T, Jul 31, 2012
- Computer Matching Act: OMB and selected Agencies Need to Ensure Consistent Implementation GAO-14-44, Jan 13, 2014
- Best Practices: Elements of a Federal Privacy Program, Federal CIO Council Privacy Committee, Jun 1010
- Recommendations for Standardized Implementation of Digital Privacy Controls, Federal CIO Council, Dec 2012