U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary of Transportation

OST

Connect the DOT Application

Responsible Official

Daniel Morgan
Email: Daniel.morgan@dot.gov
Phone Number: 202-366-4308

Reviewing Official

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The US Department of Transportation developed the Connect the DOT application to streamline the collection, storage, and management of data about the Department's executive public engagements and interactions. The application automates business functions that inform the Department's leadership about the impacts these executive-level public engagements have on the Department and its goals. The application allows the Office of Public Engagement to streamline how this data is collected, stored, and managed. The application uses the data it collects to produce reports that directly support this need.

Connect the DOT is not publicly available and does not solicit information from the public. However, information is collected in the course of a meeting such as business contact information including name, organization, phone number, email address and scheduling information. This Privacy Impact Assessment (PIA) is being conducted in accordance with the E-Government Act of 2002, as the application includes contact information on members of the public.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The US Department of Transportation developed the Connect the DOT application to streamline the collection, storage, and management of data about the Department's executive public engagements and interactions. The application is managed by the Office of the Chief Information Officer and owned by the Office of Public Engagement. It is used by officials in the Office of the Secretary of Transportation and Operating Administrations (OAs) who are involved with public engagement activities. Through Connect the DOT, authorized users may upload details about public engagements such as phone calls, meetings, speeches, roundtables, discussions, and other information such as when the engagement occurred, and key topics raised or discussed during the engagement. Users may also see engagements by other officials.

Connect the DOT is not publicly available and does not solicit information from the public. However, information collected in the course of a meeting (scheduling information, contact information) is included. The personally identifiable information (PII) in Connect the DOT is maintained to track the purpose and subject of the engagement, and to potentially follow up with the engagement participants. Individuals whose information may be included in the system include those who attend a meeting or event with a senior agency official such as the Secretary, Deputy Secretary, Assistant Secretary, Operating Administrator, or their immediate offices. Once engagement information is entered, the Department uses the data it collects to produce reports and direct follow-ups, as appropriate.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families

articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Connect the DOT is not publicly available and does not solicit information from the public. However, information collected in the course of a meeting (scheduling information, contact information) is included. The personally identifiable information (PII) in Connect the DOT is maintained to track the purpose and subject of the engagement, and to potentially follow up with the engagement participants. Individuals would be aware that DOT captured their name and contact information in our electronic mail system by virtue of choosing to correspond with and interact in engagements. Information is provided voluntarily and provided for the purpose of being contacted to participate in interactions and engagements with the Department.

The Department provides general notice to the public of this records collection through its Privacy Act system of records notice (SORN), DOT/ALL16 – Mailing Management Systems (71 FR 35319 dated June 19, 2006). Records are indexed by the name of the engagement participant. In addition, this PIA, which is published on the Department's Privacy Program Web site (https://www.dot.gov/privacy/), provides additional information on the privacy risks and mitigation strategies for the system.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

Under the provisions of the Privacy Act, individuals may request searches of agency records to determine if any added records pertain to them. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Office of the Chief Information Officer

1200 New Jersey Avenue, SE

Washington, DC 20590

DOTCIO@dot.gov

(202) 366-9201

The request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records
- A signed attestation of identity

Individuals seeking to contest information about them that is contained in the Connect the DOT application should make their request in writing, detailing the reasons their records must be corrected and addressing their letter to the following address:

Departmental Privacy Officer

1200 New Jersey Avenue, SE

Washington, DC 20590

privacy@dot.gov

(202) 366-9201

Additional information about the Department's privacy program may be found at https://www.transportation.gov/privacy-program. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

Connect the DOT is integral to the operation of the Department in furtherance of its responsibilities to ensure a safe and reliable transportation system as authorized by 49 CFR. PII in Connect the DOT is maintained to track the purpose and subject of the engagement,

and to potentially follow up with the engagement participants. The purpose of the system is to provide a history of public engagement activity by senior agency officials.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

Connect the DOT only collects the information needed to accomplish its stated purpose. Connect the DOT does not require any PII from the public. However, PII voluntarily provided in the course of a public engagement activity is saved for the purpose of identifying the stakeholder and providing the option for follow-up on the agency priorities of interest to the stakeholder.

Connect the DOT also collects information about its users within the Department such as contact information, role-based authorization, and organization information. The purpose of this collection is to specifically authorize a user to access the application and to send automated notifications to the users.

Records are maintained in accordance with GRS 4.2, Information Access and Protection Records; item 130, DAA-GRS2013-0007- 0012, Personally identifiable information extracts and item 140, DAA-GRS2013-0007- 0013, Personally identifiable information extract logs and GRS 6.4, Public Affairs Records, item 020, DAA-GRS2016-0005-0002, Public correspondence and communications not requiring formal action.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

Connect the DOT collect PII and this information is not used in any manner that is not specified in notices and is only used for the purposes collected. Consistent with the Privacy Act system of records notice associated with this application, data entered and stored in Connect the DOT is used for reporting, referral to the appropriate office within the DOT, and follow-up with engagement participants. Additionally, the Department may share PII maintained in Connect the DOT for purposes stated in the Department's Prefatory Statement of General Routine Uses.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Authorized users enter data via the application. The application links with the Department's email and calendaring system to ensure consistency and accuracy of data. To preserve data quality and integrity in the event that data in the system becomes corrupt or needs to be restored, backups are performed regularly.

OST ensures that the collection, use, and maintenance of information collected for operating Connect the DOT is relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, is accurate, complete, and up-to-date.

The redress process described in this PIA is a mechanism to maintain and improve accuracy of information.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

Connect the DOT takes appropriate security measures to safeguard PII and other sensitive data. Connect the DOT applies Departmental security standards, including but not limited to routine scans and monitoring, backup activities, and background security checks of technical employees and contractors.

The DOT network is designed to protect from internet attacks and there are protective devices strategically placed throughout to prevent unwanted attacks from within the network. DOT has employed intrusion detection and prevention devices throughout the network to protect the network from many malicious codes.

Identification and Authentication safeguards require each user to positively identify themselves by a unique user identification and the Personal Identity Verification (PIV) credential prior to being granted access. These safeguards serve as the mechanism that associates a specific user with the recorded audit events. The user's PIV credential ensures proper identity, enabling the system to perform authentication. Access to any information – including sensitive information – in Connect the DOT requires a valid user identifier and PIV credential. All authorized users must agree to DOT-wide "Rules of Behavior" before being granted access to the network and, thereby, the application.

All system components are hosted within in the Microsoft Azure cloud. Physical access controls are established and documented in the Microsoft Azure FedRAMP authorization.

Accountability and Auditing

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

OST is responsible for identifying, training, and holding OST employees and contractors accountable for adhering to DOT and OST privacy and security policies and regulations. OST follows Fair Information Practice Principles (FIPPs) as best practices for the protection of PII associated with Connect the DOT. In addition to these practices, additional policies and procedures are consistently applied, especially as they relate to the protection, retention, and destruction of records.

Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual Security and privacy awareness training as well as the DOT/OST Rules of Behavior. The OST Information System Security Officer and OST Privacy Officer will conduct periodic security and privacy compliance reviews of the Connect the DOT consistent with Departmental policy requirements.

Connect the DOT inherits audit logging from the Microsoft Azure cloud. Logs are periodically reviewed for any anomalies. The System Owner, Information Systems Security Manager (ISSM) and/or Cybersecurity Management Center (CSMC) will determine the frequency and any changes which need to occur on the system due to the current threat environment. Only authorized system, database, and application administrators have rights sufficient to access audit logs based on their particular roles. The logged auditable events are adequate to support after-the-fact investigations based on previous requests made by the CSMC.

Responsible Official

Daniel Morgan
System Owner
Chief Data Officer, Office of the Chief Information Officer

Approval and Signature

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer