U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration

Stakeholder Contact Database

Responsible Official

Susan Kirinich
Management Analyst, System Manager
Office of Government Affairs, Policy and Strategic Planning
202-366-7124
Susan.kirinich@dot.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=DOT Headquarters, ou=OSTHQ, cn=CLAIRE W BARRETT
Date: 2017.11.17 16:58:00 -05'00'

Executive Summary

The U.S. Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) is responsible for reducing deaths, injuries, and economic losses resulting from motor vehicle crashes on our nation's roadways. NHTSA develops and enforces Federal Motor Vehicle Safety Standards (FMVSS), conducts research on behavioral and vehicle safety, develops traffic safety programs and countermeasures, and oversees vehicle safety defect investigations, recalls and remedies. To carry out its mission, NHTSA partners with a wide range of stakeholder organizations at the federal, State, and local levels.

NHTSA's Office of Government Affairs, Policy and Strategic Planning developed a stakeholder database that allows NHTSA to more effectively maintain contact information and manage communications with its partners. The Stakeholder Contact Database contains minimal amount of business contact information such as the name of an official contact for the organization, the contact's business email and telephone number(s), and the organization's business address. This information is used to send emails to keep stakeholders informed on NHTSA events, initiatives, or newly released publications. This Privacy Impact Assessment (PIA) is being conducted in accordance with the E-Government Act of 2002, as the database includes the professional contact information of 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:

- *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

Traffic injury prevention is a cross-cutting field involving federal, public, and private sector organizations in the transportation, enforcement, and public health arenas. NHTSA has long maintained contact information for its partners in these areas to promote better communication and to disseminate, via email, information about upcoming Administration events, initiatives, or recently released publications. This provides a way for the disparate stakeholders to stay engaged on new inititives and technical resources. Additionally, it provides a means of obtaining feedback on NHTSA programs from our partners. This dialogue strengthens these partnerships and helps shape and inform future programs and policies.

Historically, NHTSA maintained multiple lists of partner organizations and the contact information for their representatives including official email, phone, and mailing addresses, in structured and unstructured formats. These records were subject to error due to duplication, limited ability to collaborate among authorized staff, and was also highly inefficient as it did not allow NHTSA to leverage automated communication workflows and processes. In order to address these issues, NHTSA developed the Stakeholder Contact Database. The Stakeholder Contact Database stores PII in the form of business contact information that is collected by NHTSA staff engaged with the stakeholder communitity. The information is collected through various forums such as meetings and events where the registered individuals share their contact information with NHTSA, or provide NHTSA staff with contact information by sharing business cards or exchanging of contact information via email.

Employees at Headquarters and NHTSA's 10 Regional Offices will add their stakeholder contacts to the database and use the database to contact stakeholders to disseminate information about NHTSA. Using the platform's built-in security, the application defines a set of user privileges to read, edit and perform administrative functions based on granted permissions. One person per office will be designated as the Stakeholder Contact Database liaison. Each will be responsible for maintaining control of the system, maintaining and updating the contacts added to the system, and ensuring that it remains current. There is a division code that allows for tracking, and the database indicates who has made changes, which allows the Office of Government Affairs, Policy and Strategic Planning to keep track of changes by name.

The Stakeholder Contact Database technical architecture consists of a SharePoint Server front end application and Microsoft SQL back end database. The application interface provides a table that allows for the searching, filtering, and saving of data. Web part lists appear as "pop up" windows for performing system functions to maintain the stakeholder contact information, create mail-merge templates, and send email messages. The document library is a shared repository for system artifacts such as the user guide, training materials, and access materials. Email templates enable staff to create standard formats includingthe NHTSA logo, reference links, and message contents. The templates allow the users to simply select the names they want, preview the email before sending, and send. The mail-merge function automatically places stakeholder data such as name and title in the message as defined. These features enhance staff collaboration, and improve the accuracy of correspondence. Accuracy is increased in that there is less chance of including the wrong person and their email in the distribution, duplication of records will be reduced, and staff can collaborate to avoid sending duplicative emails.

Fair Information Practice Principles (FIPPs) Analysis

The Fair Information Practice Principles (FIPPs) are rooted in the tenets of the Privacy Act and are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs are common across many privacy laws and provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis DOT conducts is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v.3i, which is sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council.

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.

Individuals voluntarily provide their contact information to NHTSA via business cards and email, they are not required to provide contact information. NHTSA also reaches out and contacts new organizations directly to obtain contact information of key officials for the express purpose of adding them to the "mailing list" to send information on NHTSA activities. The new database is a transfer of the names of existing contacts into an electronic system, with new contacts being added as they are obtained. Upon system approval, an initial "welcome" email will be sent that will provide the the opportunity to unsubscribe. Stakeholders will be able to unsubscribe and have their email deleted from the database at any time by emailing the database owner or using the "unsubscribe" feature included in all emails.

NHTSA also informs the public that their PII is stored and used by the Stakeholder Contact Database through this Privacy Impact Assessment published on the DOT website. This document identifies the information collection's purpose, storage and use the PII, along with all uses of how the PII stored and transmitted.

Notice is also provided to individuals through the Privacy Act System of Records (SORN) for DOT/ALL 16 - Mailing Management System - 71 FR 35319 - June 19, 2006.[1]

Individual Participation and Redress

DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Individuals voluntarily provide their contact information to NHTSA which is then used to send information via email. Individuals are not told explicity that they will be receiving an email when they provide their business card or email. However, at any time, individuals can "opt out" and unsubscribe to have their name removed from the system. If an individual believes their information is being used outside of the scope of the purpose for the system, have a privacy concern, or a data inaccuracy concern, they can contact a responsible NHTSA staff member or write to NHTSA.Privacy@dot.gov.

Subject to the limitations of the Privacy Act, individuals may request access to information about themselves contained in a DOT system of records through DOT's Privacy Act/Freedom of Information Act (FOIA) procedures. As a matter of policy, DOT extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOT by complying with DOT Privacy Act regulations, 49 CFR Part 10. Privacy Act requests for access to an individual's record must be in writing either handwritten or typed, may be mailed, faxed or e-mailed. DOT regulations require that the request include; include a description of the records sought, the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Additional information and guidance regarding DOT's FOIA/PA program may be found on the DOT website. Privacy Act requests may be addressed to:

[1] https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/pdf/E6-9581.pdf

Claire W. Barrett
1200 New Jersey Ave., SE E31-312
Washington, DC 20590
privacy@dot.gov

Authority and Purpose

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 its collects, uses, maintains, or disseminates PII.

Congress enacted the National Traffic and Motor Vehicle Safety Act in 1966 for the purpose of reducing deaths and injuries as a result of motor vehicle crashes. Additionally, 23 U.S.C. 4 authorizes NHTSA to assist and cooperate with other Federal departments and agencies, State and local governments, private industry, and other interested parties, to increase highway safety. The Stakeholder Database will help promote highway safety among NHTSA's various partners by sharing information related to traffic injury prevention and safety.

The PII contained in the Stakeholder Contact Database, used to identify contacts in order to send out notices of upcoming Administration events or recently released publications, is in accordance with the data elements and data categories in the SORN. The information will be used solely for this purpose. The database will not be used to request or collect information from the groups about their members.

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. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The information is the Stakeholder Contact Database will be limited to basic contact information to include:

- Name of an official contact for the organization
- Contact's business email
- Telephone number(s)
- Organization's business address

The information collected is necessary to send electronic correspondence from NHTSA. Information that is not relevant or required to send correspondence, such as date of birth, will not be collected or included in the database.

The contact information will be updated on a monthly basis when we find that the email addresses are no longer valid or if a contact is to be removed from the system. The information retained is for points of contact within organizations, not individual researchers. While the information is on individuals, NHTSA is interest is to maintain contact with relevant organizations. As such, when an individual leaves an organization or changes positions, their contact information will be deleted and replaced the person that takes over the role. The retention of the contact information will be on an ongoing basis until such time as either an individual or organization requests to be removed, or the contact information is no longer accurate. Additionally, any individual may opt out of any distribution list at any time in order to have their information expunged from the Database...

The Database is scheduled under GRS 6.5, item 20, "Public Customer Assistance Records, item 20, Customer/client records"[2] which includes distruntion lissts used by an agency to deliver specific goods or services. Records include; contact information for customers or clients, subscription databases for distributing information such as publications and data sets produced by the agency, files and databases related to constituent and community

[2] https://www.archives.gov/files/records-mgmt/grs/grs06-5.pdf

outreach or relations, and sign-up, request, and opt - out forms. Records are may be deleted when superseded, obsolete , or when customer requests the agency to remove the records.

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.

The information in the system is collected to facilitate dissemination of information to NHTSA's partners. The contact information will only be used within the scope of the purpose, it will not be used for any other reason. The information in the database will not be shared with any outside entity or third-party organization. Access to the Datbase is limited to a certain number of people within NHTSA, and the Database has access controls that will be monitored.

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).

NHTSA ensures that the use and maintenance of information collected for operating the Stakeholder Contact Database is relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, that it is accurate, complete, and up-to-date throughout the record lifecycle. Information is collected directly from individuals who volunteer information, usually in the form of business cards, and is assumed to be accurate. The information is entered manually by the NHTSA employee via the SharePoint site. If an email is returned as undeliverable, it will be forwarded to the office management and the person who enters the information can update or delete the contact from the system. Each office that enters data will be responsible for ensuring its accuracy. As contact information changes, the office will update it on a monthly basis.

The Stakeholder Contact Database has its own internal process for ensuring that only authorized users can gain access, and obtain permission to perform certain functions, and maintain a single authoritative source. The system provides version control to record data changes, email preview to verify content prior to sending, and retains a history of sent emails.

Security

DOT shall implement administrative, technical, and physical measures 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.

Records in the Stakeholder Contact Database are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. A user guide and training documentation specific to the Stakeholder Contact Database is published on the DOT Sharepoint page. Access to the DOT/NHTSA Sharepoint site containing the records in the Stakeholder Contact Database is limited to those individuals on a need-to-know basis for the performance of their official duties, and who have appropriate clearances and permissions. All records in the Stakeholder Contact Database are protected from unauthorized access through appropriate administrative and technical safeguards. Utilizing built-in security, the application also defines a set of user privileges to determine and limit who can read, edit and perform administrative functions based on granted permissions.

Accountability and Audit

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.

NHTSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to NHTSA privacy and security policies and regulations. NHTSA will follow the FIPPs as best practices for the protection of information associated with the Stakeholder Contact Database. In addition, these practices, policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees will be given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance will be provided in the form of mandatory annual Security and privacy awareness training consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Audit provisions are also included to ensure that the Stakeholder Contact Database is used appropriately by authorized users.

Responsible Official

Susan Kirinich
Management Analyst
Office of Government Affairs, Policy and Strategic Planning

Approval

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer