U.S. Department of Transportation

Privacy Impact Assessment (PIA)

Federal Transit Administration (FTA)
Public Transportation Agency Safety Plans (PTASP)

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
Date: 2019.12.17 22:01:58 -05'00'

Executive Summary

The mission of the Department of Transportation's Federal Transit Administration (FTA) is to improve public transportation for America's communities. The FTA provides financial and technical assistance to local public transit systems, including buses, subways, light rail, commuter rail, trolleys and ferries. FTA also oversees safety measures and helps develop next-generation technology research. The Public Transportation Safety Plan Final Rule, 49 C.F.R. Part 673 requires FTA to establish a web forum for individuals to ask questions about and comment on ideas concerning the development and implementation of Public Transportation Agency Safety Plans (PTASP). In order to fulfill this requirement, FTA's Office of Transit Safety and Oversight (TSO) is using the Department of Transportation's Idea Forum, www.usdot.uservoice.com, to establish the Public Transportation Agency Safety Plans (PTASP) Technical Assistance Center (TAC). The PTASP TAC will allow any interested party to provide ideas and feedback on the development and implementation of PTASP. Feedback and ideas submitted through the PTASP TAC will be considered in the development of public transportation safety plans, but will not be legally binding and will not be relied upon by FTA as a separate basis for affirmative enforcement action or other administrative penalty.

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.

[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).

Introduction & System Overview

The FTA's Office of Transit Safety and Oversight (TSO) Public Transportation Agency Safety Plans Technical Assistance Center (PTASP TAC) is a web forum for individuals to submit comments and ideas on key questions concerning the development and implementation of, as required in 49 C.F.R. Part 673.

Moving Ahead for Progress in the 21st Century Act (MAP-21) is a funding and authorization bill governing United States federal surface transportation spending. The establishment of Public Transportation Agency Safety Plans (PTASP) was required by the implementing regulation found at 49 C.F.R. Part 673. While participation is voluntary, any covered transit agency, State Department of Transportation, State Safety Oversight Agency (SSOA), local governmental entity, contractor or other interested party is encouraged to participate in FTA's PTASP TAC. Guidance provided through the PTASP TAC is not legally binding and will not be relied upon by FTA as a separate basis for affirmative enforcement action or other administrative penalty.

User Access to PTASP

PTASP TAC leverage's the DOT's Office of the Chief Information Officer's (OCIO) Idea Forum powered by UserVoice. After accessing the Idea Forum home page (https://usdot.uservoice.com) users may select the link to the PTASP TAC site. Once there, users are requested sign-in or create a new account. To register, users are only required to provide an email address. This email is used to provide correspondence with the user, but is not required to be verified by the user, thus a user could provide a dummy email account in order to remain anonymous. Users can create an avatar by creating a "Gravatar" from a third-party source. (https://en.gravatar.com/). Once a Gravatar is connected to the email address the user registers with it, it will then automatically populate. Language can be specified in the account settings page. PTASP TAC also allows users access through Facebook and Google. OCIO whose Sharepoint site hosts the PTASP TAC site has an backend account (administrative privileges) to the database. FTA personnel in the TSO office also have access to the backend account.

Using PTASP

Once the user account is created, the user can change how their account is displayed in the forum by modifying their settings. Settings are accessed by clicking the settings link. Once in the settings menu, users may edit their display name, email, and language. Users may also post a new idea or comment on a current forum post. To post a new idea, the user simply clicks on the "Post a new idea" link found in the technical assistance forum section of the main page. To comment on a forum post, the user may either select a recently updated idea from the main page, search for a topic using the search bar, or enter one of two pre-established feedback forums found on the main page.

In addition to posting ideas or comments, users can also create a new forum post by clicking in the box labeled "Do you have a PTASP question or suggestion". If a user has signed in, the username will automatically post from their profile. If they have not signed in, the user will be prompted for their email address. Once the question is entered, it will automatically display so that the user will be able to review it. The user may then choose to submit it or to return to the previous page. If the user submits the post, it will be sent to the administrative team for review and approval prior to posting. If the post is on topic and not offensive, the administrative team will promote it so that it may be viewed by all users. To comment on an existing post, the user must select a post from the forum main page. Once accessed, the user can post a reply using the add comment box. If a user has signed in, the username will automatically post from their profile. If a user is not signed in, the user will be prompted for their email address. Once submitted, the post will be sent to the administration team for review and approval under the protocol listed above prior to posting. Users can also access and view suggestions and comments from registered users without signing in.

Personally Identifiable Information in PTASP

Users are required to provide an email address for system registration and access. The email address is used by FTA to correspond with the user. The name and email address information provided will be retained by the system. FTA may need to correspond with the user to verify information provided in a comment or question in order to prevent confusion in a forum post. FTA may also want to follow up with a user to ensure their question or comment was addressed sufficiently. If a user chooses to respond to a question, the information before the @ (user's name or alias) is used to log the user's response, and will be displayed by the system. For example, "privacy@transportation.gov" would be displayed as "privacy". Although comments posted to the forum are moderated, user accounts are not verified.

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.

FTA clearly discloses its policies and practices concerning all PII collected, maintained, used, and disseminated. FTA will provide notice to individuals through DOT's UserVoice's privacy notice. The UserVoice privacy notice is found in the Terms of Service. Users of the system will be made aware that they can also provide feedback anonymously. To provide feedback anonymously, navigate directly to US DOT landing page URL (https://usdot.uservoice.com/) or directly to each sub-forum from FTA's PTASP TAC Community of Practice web page: https://www.transit.dot.gov/PTASP-COP.

Anonymous users can view all suggestions and comments. Although users do not have to provide a name in order to comment, users must provide an email address. User are not required to register and may provide any email they would like (including fictitious ones) in order to register.

Users of the system will be able to delete their profile if they choose to do so; however, previously submitted comments or suggestions will remain visible. Per its privacy policy, UserVoice uses reasonable measures to protect information stored within its databases, and restricts access to such information to those employees who need access to perform their job functions, such as customer service personnel and technical staff. FTA does not store this information outside of UserVoice.

[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

The publication of this PIA further demonstrates FTA's commitment to providing appropriate transparency into the FTA's PTASP Technical Assistance Center (TAC). This PIA is available to the public at http://www.transportation.gov/privacy.

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.

FTA will ensure that individuals have the right to (a) obtain confirmation of whether or not FTA has information relating to him or her; (b) access information related to him or her within a reasonable time, cost, and manner and in a form that is readily intelligible to the individual; (c) obtain an explanation if a request made under (a) and (b) is denied and challenge such denial; and (d) challenge information relating to him or her and, if the challenge is successful, have the data erased, rectified, completed, or amended.

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. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

The information collected helps FTA track who they have interacted with regarding ASP development and which agencies may require further follow up. This also allows FTA to provide helpful and relevant responses when communicating with individuals through multiple channels (e.g., phone, email, UserVoice.

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.

Individuals exercise complete control over the information that is submitted to the PTASP TAC. Individuals can request accounts in order to comment or they may access comments made on the site anonymously. As user accounts are not verified, information may be submitted without attribution. However the name and email address used to register to PTASP TAC are retained. If a user chooses to respond to a question, the portion of the email address that appears before the "@" will be used to identify the response. Users of the system will be made aware that they can also provide non-attributable feedback. Users of the system will also be able to delete their profile if they choose to do so, however, the system will retain all submissions and continue attribute any submissions to their username.

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.

Individuals can request accounts or their responses can be nonattributable. If a system user has an account, registered names and email address information is retained. If you choose to respond to a question the information before the @ is used to log your response. Users of the system will be made aware that they can also provide feedback anonymously. Users of the system will also be able to delete their profile if they choose to do so.

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).

Individuals can request accounts or their responses can be anonymous. If you have an account, registered names and email address information is retained. If you choose to respond to a question the information before the @ is used to log your response. Users of the system will be made aware that they can also provide feedback anonymously. Users of the system will also be able to delete their profile if they choose to do so.

The individual submitting a recommendation or feedback to FTA is responsible for ensuring the accuracy of the information they provide to FTA in their submission. When they are submitting their recommendation or feedback on a previously submitted idea, they have the opportunity to validate or edit the information they have entered prior to submitting it. Once the recommendation or idea is submitted, the individual who submitted it, is not able to change the submission, but will be able to add follow-up information. The user is able to remove content once submitted, however account information will still be captured unless the user submitted information anonymously.

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.

PII is protected by reasonable security safeguards against loss or unauthorized access, destruction, misuse, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under FISMA and the information security standards issued by National Institute of Standards and Technology (NIST), including Federal Information Processing Standards (FIPS) Publication 200 and NIST SP 800-53 Revision.4, Recommended Privacy and Security Controls for Federal Information Systems. FTA in conjunction with DOT Office of the Chief Information Officer (OCIO) implement security measures to ensure the safeguarding of the information. DOT OCIO will provide adequate security safeguards for the Idea Forum, the platform on which PTASP rests.

Only FTA and DOT OCIO personnel will have access to authentication and user account information.

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.

FTA will follow the Fair Information Practice Principles for the protection of PII associated with the implementation of FTA's PTASP TAC. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. FTA and DOT policy states that only individuals with a need to know will be provided access to the PII in the system.

Responsible Official

Paulina Orchard
Program Analyst
FTA-TSO-10

Approval

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