U.S. Department of Transportation

Privacy Impact Assessment

Federal Highway Administration (FHWA)

Transportation, Fellows, Interns, and Contractor System (TFICS)

Responsible Official

Latoya Jones
Email: Latoya.Jones@dot.gov
Phone Number: 404-562-3587

Reviewing Official

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

Executive Summary

The Federal Highway Administration (FHWA), within the Department of Transportation (DOT), has been given the responsibility for enhancing the movement of people and goods from one place to another, while also ensuring the safety of the traveling public, promoting the efficiency of the transportation system, and protecting the environment.

In support of FHWA's mission, the Office of Human Resources Talent Development Division manages the Transportation, Fellows, Interns, and Contractor System (TFICS). The TFICS aims to attract qualified students to the field of transportation education and research and advance transportation workforce development. The TFICS includes three fellowship categories including the Graduate Fellowships, Local Competition, and Grants for Research.

This Privacy Impact Assessment (PIA) is published in accordance with the E-Government Act of 2002 because the FHWA collects Personally Identifiable Information (PII) on members of the public who apply for scholarships, graduate fellowships, internships, and grants for research.

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

TFICS is a web-based portal used to collect, manage, and track applications for the Dwight David Eisenhower Transportation Fellowship Program (DDETFP). The Fellowship provides funding for students to pursue master's or doctoral degrees in transportation-related disciplines. The goals of these grants are to 1) attract the Nation's brightest minds to the field of transportation, 2) enhance the careers of transportation professionals by encouraging them to seek advanced degrees, and 3) bring and retain top talent in the transportation industry of the United States (U.S.).

The DDETFP is an annual program and information on how to apply is posted through a notice of funding opportunity on Grants.gov when the award cycle opens. The fellowship program is open to qualified students pursuing a transportation related degree at an accredited university in the U.S. Categories of Fellowships include:

- DDETFP Graduate Fellowship - provides funding for students to pursue master's or doctoral degrees in transportation-related disciplines.
- DDETFP Local Competition - encourages institutions of higher education (IHE) that are minority serving institutions and community colleges to apply for administering a DDETFP competition on their campus.
- DDETFP Grants for Research Fellowship (GRF) - structured to provide opportunities for students to work with USDOT program offices which are interested in attracting workforce-ready students pursuing advanced degrees in transportation-related disciplines.

TFICS has both internal and external users. Internal users are system owners and reviewers of DDETFP applications. External users are applicants to the DDETFP. Applicants access TFICS through FHWA's User Profile and Access Control System (UPACS) (https://www.transportation.gov/individuals/privacy/user-profile-and-access-control-system).

TFICS provides application forms for each program, as well as the interface for FHWA to manage, review, accept, reject, return, or grade the application forms.

The information in the system consists of documents related to applying to the program that include the students' name, home mailing address, email address, date of birth, academic records, home telephone number, race (optional), gender (optional), and citizenship. Use of the records maintained in the system is limited to FHWA program staff and contractors directly involved in the administration of the program and system, and to other government agencies when authorized by law.

Applicants can also upload other files that contain PII information (e.g., copy of permanent resident card, I20 documents issued by U.S. Citizenship and Immigration Services (USCIS), Resume, etc.).

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.

DOT and FHWA System of Records Notice (SORN) provide transparency about privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about individuals covered under the Privacy Act of 1974, as amended. The

[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

information in TFICS is covered by System of Records Notice (SORN) DOT/FHWA 220 - Dwight David Eisenhower Transportation Fellowship Program 73 FR 48008.

For direct access to TFICS, users must read and agree to the Terms and Conditions of Use and Rules of Behavior for a User. A warning message that discusses the penalties of unauthorized access appears before logging on. The TFICS has a link to the DOT Privacy Policy that contains all the protection and advisories required by the E-Government Act of 2002. The Privacy Policy describes DOT information practices related to the online collection and the use of PII.

The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into TFICS.

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.

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.

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 found in 49 CFR Part 10. Privacy Act requests for access to an individual's record must be in writing (either handwritten or typed), and may be mailed, faxed, or emailed. DOT regulations require that the request 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 (https://www.transportation.gov/privacy). This is accomplished by sending a written request directly to:

Federal Highway Administration
Attn: FOIA Officer (HATS-20)
1200 New Jersey Avenue SE Washington, DC 20590

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 purpose of TFICS is to collect applications to make a determination for the DDETFP. Information submitted by the applicant is used by FHWA to evaluate a candidate's ability to meet federal transportation workforce recruitment and development goals. Records contained in the system are only used for program analysis and evaluation purposes.

This information includes student names, home mailing addresses, telephone numbers, email addresses, dates of birth, race, gender, citizenship, and academic records.

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.

FHWA collects, uses, and retains only data that is relevant and necessary for the specified purpose of which it was originally collected in TFICS. TFICS retains and disposes of information in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS).

These records are retained and disposed of in accordance with NARA General Records Schedule 4.1, item 10; Disposition Authority DAA-GRS-2013-0002-0016, "Tracking and control records. Records used to provide access to, and control of records authorized for destruction by the GRS or NARA-approved records schedule. Disposition: Temporary. Destroy when no longer needed."

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.

TFICS does not use PII for any secondary purposes that might require consent unless otherwise authorized by law.

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).

TFICS collects PII directly from applicants to the DDETFP during the registration and application process. The applicant has the opportunity to review and correct information they entered. If corrections are required, the applicant can log into their application to make corrections before submittal of their application for review. TFICS also conducts address verification, input validation, and a security scan of uploaded documents.

The FHWA ensures that the collection, use, and maintenance of information collected for operating the TFICS is relevant to the purposes for which it is to be used and to the extent necessary for those purposes; it is accurate, complete, and up to date. TFICS stores and collects PII via UPACS. Users can change their personal information, and request removal of their account access from FHWA and TFICS.

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.

FHWA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, dated December 2020.

All PII is encrypted in transit and at rest. Personnel receive guidance on their duties as they relate to collecting, using, processing, and securing PII. This includes mandatory annual security and privacy awareness training, as well as a review of the DOT Rules of Behavior. The DOT and FHWA Privacy Offices conduct periodic privacy compliance reviews of TFICS with the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

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.

The FHWA identifies, trains, and holds employees and contractors accountable for adhering to DOT privacy and security policies and regulations. The FHWA follows the Fair Information Practice Principles as best practices for the protection of PII. In addition to these practices, additional policies and procedures are consistently applied, especially as they relate to 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 Rules of Behavior. The FHWA Information System Security Manager and FHWA Privacy Officer conduct periodic security and privacy compliance reviews of the TFICS system consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic resource.

Responsible Official

Latoya Jones
System Owner
Transportation, Fellows, Interns, and Contractors System

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.11.20 10:19:31 -05'00'