U.S. Department of Transportation

Privacy Impact Assessment

Federal Highway Administration (FHWA)

User Profile and Access Control System (UPACS)

Responsible Official

Stephanie Jackson
Email: Stephanie.Jackson@dot.gov
Phone Number: 202-366-1746

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 of 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. To meet these goals, FHWA maintains effective communication with other federal agencies, state and local organizations, and members of Congress. With privacy and security always foremost in mind, as FHWA automated much of this information sharing, it also implemented strict safeguards to protect against unauthorized or unintentional information exchange. The User Profile and Access Control System (UPACS) is one system that helps FHWA accomplish this.

This Privacy Impact Assessment (PIA) is being published in accordance with the E-Government Act of 2002.

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;*

[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).

- *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

UPACS is a web-enabled system designed to perform user identification, authentication and authorization for FHWA information systems. UPACS provides access control for FHWA applications through system-generated user IDs and user-supplied passwords, Personal Identity Verification (PIV) cards with Personal Identification Numbers (PINs) for DOT employees & contractors, and Login.gov via Okta for external users Level 2 authentication. To do this, UPACS maintains a record of permissions, contact information, and other related data on each user that FHWA has determined requires access to one or more FHWA systems.

Users of UPACS include FHWA employees, select State government employees, and other FHWA partners. UPACS maintains access profiles for each user to correctly apply application access rights. When a user attempts to access an FHWA information system, UPACS interfaces with the system in question, exchanging data that the system needs to permit or refuse access. Upon logging in, users are presented with a menu of FHWA information systems they have access to.

UPACS provides some of its functionality through web services, for applications that prefer to use their own Uniform Resource Locators (URLs) as entry points for their users. The application becomes responsible to provide the front-end interface for login and password management while using UPACS web services behind the scenes to perform the real work of authenticating users. When web services are used, the user is not presented with a UPACS menu.

UPACS creates user audit logs that provide the FHWA with information regarding access attempts to adequately monitor system usage and identify possible unauthorized access incidents or security breaches.

Additionally, in an effort to reduce data duplication with other systems, FHWA uses UPACS data to provide information in accordance with predefined and acceptable uses, outside of access control such as employee telephone lists and organizational directories.

The UPACS system uses both non-personally identifiable and Personally Identifiable Information (PII) for each individual who requires access to a FHWA system. UPACS contains PII on Federal government employees and contractors, state and local government employees and contractors, members of the public, and a limited number of Congressional staff who require access to one or more FHWA systems.

The PII includes:

- First Name
- Last Name
- Business address
- Phone number
- Business email
- Secret Word
- Emergency contact information for select FHWA employees.

Users may register with UPACS two ways:

- Directly – Users can set up an account directly through the UPACS web interface.
- Indirectly – There are a few FHWA information systems that sit behind UPACS that allow users to set up accounts. Though it is transparent to the user, it creates an UPACS user account.

Accounts are approved and managed by the UPACS system administrators.

UPACS shares identification, authentication, and authorization information with other FHWA systems in order to manage access. UPACS does not share PII with any other systems.

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]*.*

[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

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 Notices (SORNs) 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 information in UPACS is covered by DOT/FHWA 219 – User Profile and Access Control System (UPACS) – 71 FR 266167.

For direct access to UPACS, 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. UPACS has a link to the FHWA Privacy Policy for UPACS and Interfaced Applications that contains all the protection and advisories required by the Privacy Act of 1974. The Privacy Policy describes FHWA and UPACS information practices related to the online collection and the use of PII.

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.

Users provide the initial data when they create their account. Users can update their account information as needed. FHWA only requests the information discussed in this document and the UPACS SORN. The information collected is not used outside of the routine uses outlined in the SORN.

Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), individuals may request searches of UPACS to determine if any records pertain to them. 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

The request must include the following:

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

Additional information and guidance regarding DOT's FOIA/PA program may be found on the DOT website (https://www.transportation.gov/privacy).

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 main purpose for UPACS is to create and manage user accounts so that individuals can access FHWA systems. FHWA uses PII within UPACS to identify user access to systems, set access permissions, monitor access, and contact users with questions and concerns. FHWA may also use some PII, such as telephone numbers of federal government employees and contractors, to publish telephone lists. If a user no longer requires access to any FHWA system, they are deleted from the UPACS database. At that point, only log files of access remain that may include information on that user.

UPACS shares PII with approximately 28 systems to manage access. All systems linking with UPACS receive data on the user's first and last name, ID, password, PIN, secret word, organization, and access rights. Some systems also receive additional UPACS data on individuals. Data sharing occurs only in pre-determined ways, based on system purpose, structure, and necessity. FWHA also publishes telephone lists for FHWA employees and contractors; these include name, telephone number, and information on hearing impairment needs for some employees and contractors. FHWA uses UPACS data to publish these telephone lists. FHWA does not share UPACS PII in any other way, except as required by law.

The UPACS system provides visible links to a Privacy Policy that describes privacy practices and information uses. In the future, UPACS may provide links to Web sites outside of DOT/FWHA. In these cases, UPACS will provide a pop-up window that informs a user that he or she is leaving the site and that different privacy practices may apply.

On registration with the system, and again annually, users must read and agree to Terms and Conditions of Use, in which UPACS monitoring and possible consequences are described.

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 purpose of UPACS. UPACS retains and disposes of information in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS).

NARA GRS 3.2, item 031 provides for the destruction of the information in the system 6 years after the user account is terminated.

At the end of the retention cycle the UPACS system administrator works with the FHWA Records Officer to properly dispose of the records per the NARA GRS.

UPACS automatically notifies the system administrator of inactive users.

- After 60 days of inactivity, the user account is soft-locked. This requires the user to reset their password the next time they login.
- After 180 days of inactivity, the user account is hard-locked. This requires the system administrator to un-lock the UPACS account and the user to reset their password the next time they login.
- After 360 days of inactivity, UPACS accounts are closed and will be deleted according to the record schedule

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 FHWA minimizes its data collection to that necessary to meet the legally authorized business purpose and mission of the Agency. FHWA uses PII within UPACS to identify user access to systems, set access permissions, monitor access, and contact users with questions and concerns. FHWA may also use some PII, such as business phone numbers of federal government employees and contractors, to publish phone lists. If a user no longer requires access to any FHWA information system or no longer needs to be included in an employee phone list, he or she is deleted from the UPACS database. At that point, only log files of access remain.

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).

The FHWA ensures that the collection, use, and maintenance of information collected for operating the UPACS 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.

Users access their own PII through the UPACS Web site, which authenticates applicants through applicant-provided online ID and password, DOT-issued PIV card or Login.Gov via Okta credentials. Users may also change their PII at any time. Users may not access or change any log files or other monitoring-related information.

Users are reminded annually to review and update their account information.

If for business reasons FHWA changes the data types that are being collected, they must follow the FHWA IT systems change management process.

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.

UPACS properly secures the information collected online by taking the following steps:

- Employ internal access controls to ensure that only people who see your information are those with a need to do so to perform their official duties;
- Train relevant personnel on our privacy and security measures to know requirements for compliance;
- Secure the areas where we hold hard copies of information we collect online;
- Perform regular backups of the information we collect online to insure against loss;
- Use technical controls to secure the information we collect online including but not limited to:
    - Secure Socket Layer (SSL),
    - Encryption,
    - Firewalls,
    - Password protections;

  - We periodically test our security procedures to ensure personnel and technical compliance;
- We employ external access safeguards to identify and prevent unauthorized tries of outsiders to hack into, or cause harm to, the information in our systems.

Tampering with FHWA's Applications is against the law. Depending on the offense, it is punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

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 UPACS system consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic resource.

Responsible Official

Stephanie Jackson
System Owner
UPACS, Federal Highway Administration

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN

Digitally signed by KARYN MARIE GORMAN
Date: 2024.05.06 16:05:03 -04'00'