U.S. Department of Transportation

Privacy Impact Assessment

Federal Highway Administration (FHWA)

National Highway Institute Web Site (NHIW)/Contract Management System (CMS)

Responsible Official

Stan Woronick
Email: stan.woronick @dot.gov
Phone Number: 202 366-5707

Reviewing Official

Karyn Gorman
Chief Privacy & Information Asset 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 highway movement of people and goods, while also ensuring the safety of the traveling public, promoting the efficiency of the transportation system, and protecting the environment. One vital component involved in reaching those goals is providing training pertaining to highway activities and ensuring that professionals and members of the public have access to the best, most accurate information. Towards this goal, the National Highway Institute (NHI) within FHWA develops and implements applicable training programs. To manage this increasingly complex task and to make the training process more accessible and useful, NHI uses NHI Web Site / Contract Management System (NHIW/CMS).

This PIA was developed pursuant to Section 208 of the E-Government Act of 2002 because the FMCSA collects, uses, and maintains PII from members of the public who participate in NHI developed training.

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

NHICMS has two primary functions with NHI being the website and CMS being the back end. The course and session data stored in CMS is displayed on NHI. The information collected via NHIW, such as customer purchases or instructor registrations, is transferred and stored in CMS, and the User Profile and Access Control System (UPACS) if it is a customer's account. UPACS is a Web-enabled system designed to set and manage appropriate access to various FHWA systems, as well as detect unauthorized access.

NHICMS is NHI's primary management information system. It is the repository of operational information for all aspects of NHI's business and is designed to aid NHI in the development, administration, and maintenance of its training events. NHICMS also maintains contracts and accounts payable, tracks sessions that are offered for each course, manages instructor and customer records, and serves as the tracking mechanism for accounts receivable invoices.

NHI is part of a publicly available web site, www.nhi.fhwa.dot.gov. Through this system, members of the public can sign up for and take NHI-developed training, link to a separate government web site (pay.gov) to pay for that training, schedule and participate in a Web conference, request to host a session, and purchase materials related to the trainings offered. Through NHICMS, the user tracks courses from concept to completion.

NHICMS uses PII data from and about members of the public who take NHI-developed training. To understand the PII data stored in CMS, we first explain how it is collected through NHI.

Users may:

• Search for available training and scheduled sessions, as well as browse general information regarding NHI and developing courses.

• Sign-up to participate in a Web conference by providing first name, last name, organization name and e-mail address.

- Register as an instructor by providing a minimum of first name, last name, and e-mail address. Other, non-required fields include middle initial, organization name and contact information, instructor bio, supervisor name, supervisor organization name and contact information.

- Register to use the Web site for controlled functions via UPACS. Controlled functions include purchasing a seat in a session, submitting a host request, purchasing material, and requesting/managing a Web conference.

After an individual user registers with NHI other features are available, including:

- Updating profiles,
- Enrolling in training,
- Ordering training materials,
- Requesting to host an instructor-led session (class), and
- Requesting to host a Web conference.

The only PII data displayed in NHI is for the web conference administrator to view the participant list for Web conferences. This list includes name, work e-mail and work phone number. Those listed sign up for a Web conference without logging into NHI.

The data collected through NHI for user accounts is stored in UPACS (https://www.transportation.gov/individuals/privacy/user-profile-and-access-control-system) and accessed via CMS. The information collected includes: first name, last name, work e-mail address, work address, and work phone number. NHI uses data submitted through NHI to administer training and deliver requested information.

To track participant records for session completion to maintain International Association for Continuing Education and Training (IACET) accreditation, NHI is required to maintain learner histories. The learner histories for FHWA participants are maintained within NHICMS. This data is manually entered into the system based on hard copy forms. This process occurs three weeks after an FHWA participant completes a session. For participants external to FHWA, CMS maintains this data from paper forms that are stored in a locked room. Both paper and electronic records schedules are the same. Only limited personnel whose job functions require access to these files have access. These files are maintained according to IACET rules and regulations. CMS contains the following PII on training participants: first name, last name, work e-mail address, work address, work phone number and training history information. To manage the instructor registration process, Instructor information is also stored in CMS. The PII data for instructors include: first name, last name, work e-mail address. Instructor work address, and work phone number may also be collected.

Authorized NHI staff has access to NHI data through CMS, with system access rights and privileges managed by the system owner. NHICMS user account information is stored in UPACS. CMS can only be accessed by authorized users who have a UPACS User ID and password.

In general, NHI collects PII to register users. The information collected is stored in UPACS and CMS, and contact information is used to communicate with participants, and track and manage the training process for individuals who have taken or will take NHI courses.

Specifically, UPACS collects through NHI:

- First Name and Last Name - to uniquely identify a user
- Work Address, Work Phone Number, and Work e-mail Address - to communicate with the user and to fulfill student requests for training and materials

Though students can purchase NHI training and materials online, the e-commerce transaction is fulfilled through a link to www.pay.gov.

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.

For both direct access and Intranet access to CMTS and NHI Web Site (NHIW), users must read and agree to the FHWA Privacy Act Notice. A warning message that discusses 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

penalties of unauthorized access appears before logging on. The CMTS and NHIW 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.

Notice is also provided to individuals through the Privacy Act System of Records Notice (SORN) DOT/ALL 027 – Training Programs – 83 FR 60960 - November 27, 2018, DOT/All 13 – Internet/Intranet Activity and Access Records – 67 FR 30758 as well as DOT/FHWA 219 - User Profile and Access Control System (UPACS) – 71 FR 26167.

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.

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 Team

1200 New Jersey Avenue SE Washington, DC 20590

At any time, a user may contact a privacy representative through the public web site (https://www.fhwa.dot.gov/privacy.cfm) and ask questions on privacy concerns. This contact information is provided in the Privacy Policy, posted visibly on the Website and in the CMTS and NHIW user's manual.

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.

CMTS is NHI's primary management information system. It is the repository of operational information for all aspects of NHI's business and is designed to aid NHI in the development, administration, and maintenance of its training events. Through CMTS, the user tracks courses from concept to discontinued stages. CMTS also maintains contracts and accounts payable, tracks sessions that are offered for each course, manages instructor and customer records, and serves as the tracking mechanism for accounts receivable invoices.

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

GRS 2.6, item 010 (authority DAA-GRS-2016-0014-0001) provides for the destruction of the information in the system after 3 years old, or 3 years after superseded or obsolete, whichever is appropriate.

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

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. Information in an identifiable form is used to provide NHI and its customers with an enhanced, efficient training process. NHI does not use PII in CMTS or the NHIW for any purposes outside of the training management process, except as may be authorized by law. The NHIW system collects PII only with express permission of users, and only for activities associated with the training process.

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 NHI 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. CMTS stores and the NHIW collect most PII via UPACS directly from individuals who register with the NHIW. Customers can change their personal information, and request removal of their account access from NHIW, CMTS, and UPACS at any time.

If a customer has provided a non-functional email address or other contact information an authorized NHI staff member contacts that customer by phone or postal letter, requesting that he or she update the information. In addition, if during the training process an authorized NHI staff member realizes that an item of PII is incorrect, he or she may request that the student change the information online.

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.

CMTS and the NHIW are housed in a facility run by FHWA staff. Physical access to these systems is limited to authorized personnel through building key cards and room-access keypads.

In addition to physical access, electronic access to PII in CMTS is limited to job function. CMTS is divided into modules and users of the system have specific access authorization to these modules based on the responsibilities of their job function.

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

Responsible Official

Stan Woronick - System Owner
Training Delivery and Customer Service Manager, NHI

Prepared by: Michael Howell (FHWA Privacy Officer)

Approval and Signature

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