U.S. Department of Transportation

Privacy Impact Assessment

Federal Highway Administration

FHWA

National Highway Institute - Blackboard

NHIBB

Responsible Official

Stan Woronick
System Owner
Email: Stan.Woronick@dot.gov

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
Karyn.Gorman@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 the National Highway Institute Blackboard (NHIBB) system.

FHWA developed and published this Privacy Impact Assessment in accordance with the E-Government Act of 2002 because Blackboard collects and maintains Personally Identifiable Information (PII) on 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:

[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

The NHIBB system is the primary Learning Management System (LMS) for delivering transportation-related learning to the transportation community within the United States. It facilitates the delivery of specialized training programs essential for modernizing and maintaining the nation's National Highway System infrastructure. NHIBB provides users with a digital course content and capabilities that enhances the traditional in-person classroom environment. NHIBB offers several core abilities, including the capability to create courses, manage and deliver course assessments, provide plagiarism prevention, and allow real-time grading of assignments. Additionally, the capacity to share, reuse, and discover learning objects offers ease of effort in building courses and engaging students. These features allow for an easy-to-use interface presented to learners. NHIBB also allows users to take long and complex courses that may span several months in an easy-to-use format.

The process for establishing a NHIBB account and accessing and completing courses differ based on whether the user is U.S. Department of Transportation (DOT) staff, both Federal and Contractor, or outside of DOT. All NHIBB users outside of DOT and FHWA are authenticated using Login.Gov. DOT staff, both Federal and Contractor, use the Federal Aviation Administration's (FAA) "MyAccess" in conjunction with their government-issued Personal Identity Verification (PIV) Card. Access to NHIBB modules is managed by roles, which are established by standardized procedures and created by the System Owner (or designated representative). Each role's access to specific system modules is set by NHI Staff with the "System Administrator" role. A user can be given access to one or more modules (or specific functions within a module) depending on the user role. Users without an NHIBB account may view the course catalog, as well as self-register for a Blackboard account.

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

- Updating profiles

- Enrolling in training, both web-based and instructor-led
- Requesting to host an instructor-led session (class) and
- Requesting to host a technology-supported, virtual instructor-led course section

The PII data displayed in NHIBB to course hosts is limited to information required to deliver both instructor, and technology-supported, virtual training courses. The data collected through NHIBB for user accounts includes:

- First Name and Last Name
- Work E-mail Address
- Work Address
- Work Phone Number

NHI uses data submitted through NHIBB 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 NHIBB. This data can either be manually entered into the system based on electronic forms or updated automatically based on completion criteria established by course instructors (in cooperation with NHI). For FHWA participants, this is done within the system based on the previously mentioned completion criteria, or upon receipt of electronic forms provided by the instructor. Participants external to FHWA are handled in a similar manner, with NHI maintaining electronic records that are stored in a controlled, access limited shared drive. Only limited personnel whose job functions require access to these files have access. These files are maintained according to IACET rules and regulations. The training records contain 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 NHIBB. 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.

Data is exchanged with Pay.gov to complete electronic payments for courses and course material. During this exchange of information, the following is provided to Pay.gov: Agency_id - unique identifier of the agency already configured in Pay.gov, Payer_name- name of the payer, Payment_type. Users purchasing courses and/or course material have the option of paying via debit, credit, or ACH payments connected to their banking account. Pay.gov is solely responsible for the collection and storage of payee information. NHI-Blackboard does not directly collect or store payee information.

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 information in NHIBB is covered by System of Records Notice (SORN) DOT/ALL 27, Training Programs, 83 FR 60960 (November 27, 2018) and the DOT/ALL 13 – Internet/Intranet Activity and Access Records – 67 FR 30757 – May 7, 2002.

For direct access to NHIBB, 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 NHIBB 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 online collection and the use of PII.

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

[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

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 Officer (HATS-20)
1200 New Jersey Avenue SE Washington, DC 20590

Individuals may also submit a request online via the DOT Public Access Link (PAL) at https://pal.dot.gov/. Requests submitted through these electronic channels must include a digital certification of identity.

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 NHI is the technical training organization of the FHWA. NHI provides leadership and resources for the development and delivery of training and education programs to improve the quality of our Nation's roadways and bridges, as well as its intermodal connections. NHI also develops and administers transportation-related training and education programs that assist in applying new technologies to the planning, design, construction, and rehabilitation of our Nation's transportation infrastructure.

The National Highway Institute was established by Congress under the Federal-Aid Highway Act of 1970 (codified at 23 U.S.C. § 504) to provide training and education for the surface transportation community to improve the quality of the Nation's roadways and bridges.

NHI courses are instrumental in developing core competencies and new skills of the surface transportation workforce and in transferring leading technology and current policies in the U.S. and abroad. NHI is an integral part of the Office of Administration (HAD) of the FHWA, which reports directly to the Administrator.

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, but longer retention is authorized if required for business use.

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 NHIBB for any purposes outside of the training management process, except as may be authorized by law. The NHIBB 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 NHIBB 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.

NHIBB users are responsible for ensuring the accuracy of their information when they create their profile, which shares the user's name, physical address, email address, and phone number with Blackboard. The user can review their profile information as entered for accuracy at that time.

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.

The 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 the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 2020 (includes updates as of Dec. 10, 2020). Blackboard undergoes the FHWA information systems Security Assessment and Authorization (SA&A) process.

Blackboard implements administrative, technical, and physical measures to protect PII against loss, unauthorized access, or disclosure. Specifically, Blackboard takes the following steps to safeguard PII: identification and authentication, physical security, roles and permissions, and encryption. Physical security includes physical access and environmental controls for the building that houses the Blackboard servers. Blackboard manages access to information through FHWA user roles. All Blackboard users must agree to the Rules of Behavior, which emphasize privacy protective practices, such as not posting PII on Blackboard, before they can access each course. Blackboard also securely transmits online learner information using encryption. The Blackboard user profile webpage, where a student accesses their account, uses an encrypted link between a student's web browser and

Blackboard. Additionally, all online learner information maintained in Blackboard is encrypted.

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 Programs Manager
Office of Innovation Management, Education, and Partnerships
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: 2026.05.14 12:40:31 -04'00'