# U.S. Department of Transportation

# Privacy Impact Assessment

**Federal Motor Carrier Safety Administration**
**Office of Analysis, Research and Technology**
**North American Fatigue Management Program (NAFMP)**

## Responsible Official

Theresa Hallquist
NAFMP Program Manager
FMCSA Research Division
theresa.hallquist@dot.gov

## Reviewing Official

Claire W. Barrett
Chief Privacy & Information Governance Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=CLAIRE W BARRETT
Date: 2018.04.12 14:01:10 -04'00'

## Executive Summary

The U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) core mission is to reduce commercial motor vehicle-related crashes and fatalities. FMCSA's Office of Research,on behalf of the North American Fatigue Management Program Steering Committee (SC), maintains the North American Fatigue Management Program (NAFMP) which enhances the safety of the commercial motor carrier industry through research and resulting best practices that address operator fatigue. NAFMP maintains a publically accessible web-based training environment to educate the public, specifically drivers and motor carrier employees, about the dangers of fatigued driving and best practices to avoid fatigue while on duty. This Privacy Impact Assessment (PIA) was conducted because the NAFMP training environmentcollects Personally Identifiable Information (PII) necessary to register users.

## 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.*

## Introduction & System Overview

The North American Fatigue Management Program (NAFMP) is a collaborative initiative led by a consortium of government and industry agencies with an interest in developing a more effective means of dealing with professional driver fatigue. The purpose of the NAFMP is to address the issue of driver fatigue with a comprehensive approach that includes: information on how to develop a corporate culture that facilitates reduced driver fatigue; a fatigue management education for drivers, drivers' families, carrier executives and managers, shippers/receivers, and dispatchers; and information on sleep disorders screening and treatment. The NAFMP will be effective in reducing driver fatigue through increased awareness and recognition of the impact of fatigue on driver safety performance; provision of training, education and motor-carrier best practices regarding how drivers

[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).

can better manage their lifestyles and how carriers can effectively support them; the identification of factors related to sleep disorders, screening and treatment; guidance on technology used in fatigue monitoring and supply chain scheduling. The NAFMP is free and available to the public. Although the use of the NAFMP is not mandatory, carriers can adopt the materials as they see fit for their companies. In addition, drivers can take training to enhance their knowledge of driver fatigue.

The NAFMP instructional program consists of a series of ten modules systemically enabled by three technological components: a content management using an open source platform website creator (e.g. Joomla); a learning management using an open source learning platform (e.g. Moodle); and a data storage using an open source database product (e.g. MySQL). The data storage component is only accessible to FMCSA and the third party contractor which maintains the system. Previously the website was hosted by the NAFMP Steering Committee (SC), but the website is now hosted by FMCSA.

The NAFMP website is provided free of charge and available for use on a voluntary basis by drivers and motor carriers worldwide. The learning modules are enhanced with full narration in both French and English, and will be supported by a Learning Management System which facilitates interactive learning whereby users will have the opportunity to test their understanding as they proceed through the material.

**Personally Identifiable Information (PII) and the NAFMP Website**

To support the fatigue management training, the system requires first time users to create a new account by registering a user name and password, email address, first name, surname, city/town, and country. Upon completion a confirmation email is sent to the registrant directing the user to the learning management system (LMS) so they can begin their courses.

The LMS tracks user progress in each training module. Upon reentry into the learning management component and reselection of the course the system returns the user to the last completed module and page.

## Fair Information Practice Principles (FIPPs) Analysis

*The DOT PIA template 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.*

[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

FMCSA informs the public that their PII is stored and used by the NAFMP website through this Privacy Impact Assessment, published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, along with all uses of the PII stored and transmitted through the NAFMP website. The NAFMP Website PIA is available to the public at http://www.dot.gov/individuals/privacy/privacy-impact-assessments.

The NAFMP does not create a new Privacy Act system or modify an existing Privacy Act system of records. PII is not retrieved by name or any other personal identifier.

The NAFMP LMS provides a Privacy Act Notice to individuals before being asked to provide personal information about themselves. as required by 5 U.S.C. §552a (e) (3).

## 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.*

PII is collected directly from individuals when they create an account for the system. This information is required to provide log in capabilities and for the user to print a customized completion form. The system also records the user's progress in each module allowing the individual .

During the account enrollment, the NAFMP asks for the user's choice to subscribe to the training and to receive certification. This dialogue asks the user to provide username, password, email address, first name, surname, city/town, and country.

The NAFMP provides an option for a user to disenroll from the system which results in a termination of account. Once the account is terminated, the individual's PII including training history is deleted.

Individuals may send an electronic message to the system administrator using the XXXX to correct or amend their PII information as needed.All PII is provided directly from the user and at any point the user can log into his or her account to view the information they provided.

## 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 its collects, uses, maintains, or disseminates PII.*

The NAFMP was developed to provide motor carriers and their employees with a program for Fatigue Management and to allow individuals to access the training modules. PII is collected directly from individuals when they create an account for the system. This information is required to provide log in capabilities and for the user to print a customized completion form. The system also records the user's progress in each module.

The city/town and country field is collected from users to determine where the users of the system are located in a general sense. The NAFMP was developed by a group of people from the U.S. and Canada with a goal to reduce fatigue related incidents. Detemining where users are from allows for underserved communities to be identified and informed about the training availibility.

## 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. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.*

The NAFMP system gathers only the information essential to establish a training user account (username, password) and information necessary to track completion of training (first name, surname, city/town, and country, and email address) for the life of the program at FMCSA. As FMCSA will maintain the project for 18 months, the information will be deleted after 18 months.

FMCSA only uses and retains data that are relevant and necessary for the purpose of the NAFMP systemin accordance with the National Archives and Records Administration (NARA) General Records Schedule 3.2 Information Systems Security Records, item 030 and 031.

## 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 NAFMP system limits the use of user collected information, namely username, password, city/town, and country explicitly to to establish an account and track completion of training.

## 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).*

All PII is collected directly from individuals when they create an account for the system. During the account enrollment, the NAFMP asks for the user's choice to subscribe to the training and to receive certification. This dialogue asks the user to provide username, password, email address, first name, surname, city/town, and country. All PII is provided directly from the user and at any point the user can log into hir or her account to view the information they provided. FMCSA relies on the user to provide and ensure his or her PII is accurate and complete.

## Security

*DOT shall implement administrative, technical, and physical measures 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, usage, modification, or disclosure. These safeguards incorporate standards and practices required for Federal information systems under the Federal Information System 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 NIST Special Publication (SP) 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013. FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII

- Protect against unauthorized access to or use of PII

Records in the NAFMP system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems' security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in the NAFMP system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All records in the NAFMP system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the NAFMP system is logged and monitored.

The NAFMP system maintains an auditing function that tracks all user activities in relation to data including access and modification. FMCSA prevents unauthorized access to data stored in the NAFMP system through technical controls including firewalls, intrusion detection, encryption, access control list, and other security methods. These controls meet Federally mandated information assurance and privacy requirements.

FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training and role-based training offered by DOT/FMCSA. This training allows individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use PII in the course of performing their duties. No access will be allowed to the NAFMP system prior to receiving the necessary clearances and security and privacy training as required by DOT/FMCSA.

A security authorization is performed every year to ensure that the NAFMP system meets FMCSA and Federal security requirements. The NAFMP system also undergoes an additional security authorization whenever a major change occurs to the system. The NAFMP system is assessed in accordance with the Office of Management and Budget (OMB) Circular A-130 Appendix III, Security of Federal Automated Information Resources, and the DOT Certification and Accreditation Guidance. The NAFMP system is approved through the Security Authorization Process under the National Institute of Standards and Technology.

**Security Assurances Inherited from the AWS Cloud**

Use of the AWS Cloud allows FMCSA to re-use and leverage a FedRAMP-compliant cloud system environment and approved Federal cloud service provider (CSP). The AWS FedRAMP-compliant environment consists of the AWS Cloud network and AWS internal data center facilities, servers, network equipment, and host software systems that are all under reasonable control by AWS. The AWS Cloud environment and service facilities are restricted to US personnel, and all AWS Cloud community customers are restricted to US government entities from Federal, state or local government organizations.

The AWS environment has been evaluated and tested by FedRAMP-approved independent third-party assessment organizations (3PAOs). The AWS is designed to meet NIST SP 800-53 minimum security and privacy control baselines for information and/or Federal information systems' risk up to Moderate impact levels. As confirmed through audit, the AWS addresses recent requirements established by NIST SP 800-171 for Federal agencies to protect the confidentiality of controlled unclassified information in non-federal information systems and organizations. AWS provides FIPS Pub 140-2-compliant services to protect data-at-rest with AES-256-based encryption and validated hardware to secure connections to the AWS.

## 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.*

FMCSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA follows the Fair Information Principles as best practices for the protection of information associated with the NAFMP system. In addition to these practices, 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 data. Guidance will be provided in the form of mandatory annual Security and privacy awareness training as well as DOT/FMCSA Rules of Behavior. The FMCSA Security Officer and FMCSA Privacy Officer conduct regular periodic security and privacy compliance reviews of the NAFMP system consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Audit provisions are also included to ensure that NAFMP is used appropriately by authorized users and monitored for unauthorized usage. All FMCSA information systems are governed by the FMCSA Rules of Behavior (ROB) for IT Systems. The FMCSA ROB for IT Systems must be read, understood, and signed by each user prior to being authorized to access FMCSA information systems, including NAFMP.

## Responsible Official

Theresa Hallquist
NAFMP Program Manager
FMCSA Research Dvision
theresa.hallquist@dot.gov

## Approval and Signature

Claire W. Barrett
Chief Privacy & Information Governance Officer
Office of the Chief Information Officer
privacy@dot.gov