U.S. Department of Transportation

Privacy Impact Assessment (PIA)

Federal Motor Carrier Safety Administration (FMCSA)

Training Provider Registry (TPR)

Responsible Official

Nikki McDavid
Email: Nikki.McDavid@dot.gov
Phone Number: 202-366-0831

Reviewing Official

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

Executive Summary

The Department of Transportation's (DOT) Federal Motor Carrier Safety Administration (FMCSA) developed the Training Provider Registry (TPR) under the authority of Section 32304 of the Moving Ahead for Progress in the 21st Century Act (MAP-21). Section 32304 of MAP-21 requires FMCSA to establish minimum training requirements for entry-level drivers. The TPR is a national database comprised of training providers who provide instruction to entry-level drivers and those seeking commercial driver's license (CDL) endorsements or upgrades. FMCSA published the Minimum Training Requirements for Entry-Level Commercial Motor Vehicle Operators final rule[1] establishing minimum training standards for certain individuals applying for their CDL for the first time; an upgrade of their CDL (e.g., a Class B CDL holder seeking a Class A CDL); or a hazardous materials (H), passenger (P), or school bus (S) endorsement for the first time. These individuals are subject to the Entry-Level Driver Training (ELDT) requirements and must complete a prescribed program of instruction provided by an entity listed on FMCSA's TPR.

FMCSA is publishing this Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 to address the privacy risks associated with the TPR system and its collection and use of Personally Identifiable Information (PII).

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.[2]

[1] See 81 FR 88732 (Dec. 8, 2016) https://www.federalregister.gov/documents/2016/12/08/2016-28012/minimum-training-requirements-for-entry-level-commercial-motor-vehicle-operators

[2]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).

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

FMCSA's primary mission is to reduce crashes, injuries, and fatalities involving large trucks and buses. This mission is accomplished by developing and enforcing data-driven regulations that balance motor carrier safety with industry efficiency; using Federal and State safety information systems to focus on high-risk carriers and drivers to enforce safety regulations; targeting educational messages to carriers, commercial motor vehicle (CMV) drivers, and the public; and partnering with stakeholders (e.g., Federal, State, and local enforcement agencies); the motor carrier industry; safety groups; and organized labor) to reduce bus- and truck-related crashes.

With limited exceptions, beginning on February 7, 2022[3], all entry-level drivers must comply with the requirements of 49 CFR Part 380. At that time, individuals applying for their commercial driver's license (CDL) for the first time; an upgrade of their CDL (e.g., a Class B CDL holder seeking a Class A CDL); or a hazardous materials (H), passenger (P), or school bus (S) endorsement for the first time must complete driver training from a provider listed on the TPR.

The TPR database is comprised of training providers who provide instruction to entry-level drivers and those seeking CDL endorsements or upgrades. Training providers are required to establish accounts in the TPR including a self-certification that they meet the applicable eligibility requirements listed in §380.703(a) and agree to electronically transmit completed

[3] See 85 FR 6088 (Feb. 4, 2020) https://www.federalregister.gov/documents/2020/02/04/2020-01548/extension-of-compliance-date-for-entry-level-driver-training

Training Provider Registration Forms (TPRF) and affirming, under penalties of perjury, that the provider will teach the FMCSA-prescribed curriculum appropriate for the CDL class or endorsement, before offering training to prospective drivers. Upon registration, FMCSA issues a unique TPR number to the provider. If a training provider has more than one campus or training location, the training provider must electronically transmit an Entry-Level Driver Training Provider Registration Form for each campus or training location to obtain a unique TPR number for each location.

Once registration is complete, FMCSA publishes the provider's name, location, and contact information on the Training Provider Registry website (https://tpr.fmcsa.dot.gov/). Driver-trainees use the website to identify authorized training providers[4].

Peonally Identifiable Information (PII) and TPR

The entry-level driver training (ELDT) regulations in 49 CFR Part 380 are applicable to training providers wishing to provide ELDT and to individuals subject to the ELDT regulations. The regulations require training providers be listed on the TPR and that they electronically transmit a trainee's ELDT registration form and ELDT training certification information to FMCSA via the TPR website. Training providers, as defined in 49 CFR 380.605, include, but are not limited to, training schools, educational institutions, rural electric cooperatives, motor carriers, State/local governments, school districts, joint labor management programs, owner-operators, and individuals.

The TPR system collects information from training providers as part of the registration process. Training providers must provide the following information in their TPRF:

- Contact Information/Place of Business (mail address and/or physical location where training will be provided)
    - Training provider's legal name
    - Training provider's doing business as (DBA) name
    - Training provider's location
    - Training provider's mailing address
    - Training provider's principal telephone number
    - Training provider's principal fax number
    - Training provider's email address
    - Training provider's website address

[4] Providers who do not intend to make their services available to all driver-trainee applicants may opt-out of including their contact information on the FMCSA public website. This option will be made available at the time of initial registration and may be changed at any time by the provider. Training providers who do not wish to be contacted by driver-trainee applicants will be listed on the TPR website simply by name, city, and state.

- Additional information
  - TPR Identification Number (if applicable)
  - U.S. DOT Identification Number (if applicable)
  - Federal Transit Administration, National Transit Database (NTD) Transit Agency Identification Number (if applicable)
  - U.S. Department of Education, National Center for Education Statistics (NCES), Public School NCES District Identification Number (if applicable)
  - Name(s) of Authorized Signing Official(s)
- User Account information:
  - Legal Name
  - Location of Business
  - Mailing address
  - Name(s) of Authorized Signing Officials

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[5], 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[6].

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.

[5] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[6] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

The FMCSA does not secretly collect or store PII. The FMCSA clearly discloses its policies and practices concerning the PII collected and held associated with the implementation of this system. The FMCSA provides notice to individuals through a layered approach including the FMCSA website at www.fmcsa.dot.gov, the TPR website, and this PIA published on the DOT's privacy program's website at www.transportation.gov/privacy. This document identifies the information collection's purpose, FMCSA's authority to store and use the PII, and all uses of the PII stored and transmitted through the TPR.

Records in TPR are retrieved by the individual's name and other personal identifiers and are subject to the provisions of the Privacy Act. FMCSA maintains these records in accordance with the Department's published System of Records Notice (SORN), DOT/FMCSA 012, Entry-Level Training Provider Registry (TPR) – 86 FR 34116, June 28, 2021. The SORN provides notice as to the conditions of disclosure and FMCSA's routine uses for the information collected in the system. The SORN also requires that any dissemination of information maintained within the system be compatible with the purpose for which the information was originally collected. In addition, FMCSA issued press releases, posted information on the TPR website (https://tpr.fmcsa.dot.gov/), sent emails via a TPR listserv, provided periodic updates at industry outreach events, and posted information related to the TPR on various social media outlets.

The publication of this PIA further demonstrates FMCSA's commitment to providing appropriate transparency into the TPR. This PIA is available to the public on the DOT website at http://www.dot.gov/privacy.

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.

FMCSA ensures that individuals have the right to (a) obtain confirmation of whether or not FMCSA has PII relating to him or her; (b) access the PII related to him or her within a reasonable time, cost, and manner and in a form that is readily intelligible to the individual; (c) obtain an explanation if a request made under (a) and (b) is denied and challenge such denial; and (d) challenge PII relating to him or her and, if the challenge is successful, have the data erased, rectified, completed, or amended.

Training providers who register with the TPR have access to review their information stored in the TPR. These training providers can view their record as often as they wish at no charge.

Drivers also have access to view their information stored in the TPR. These drivers can view their record as often as they wish at no charge.

FMCSA will receive data from training providers and will review the data submitted by training providers to the TPR. Drivers will not submit ELDT certification data, FMCSA suggests and has communicated via TPR webinars that training providers allow and encourage all drivers to review their information that is collected for reporting to FMCSA via the Training Certification Information form. FMCSA also allows driver-trainees to view their ELDT certification information in the TPR to further ensure the accuracy of the data. These reviews will help reduce data errors in the form that will be uploaded to the TPR and then electronically transmitted to a driver's State of record. Although FMCSA has the responsibility to ensure that the data is transmitted to the SDLA appropriately, it relies solely on the accuracy of the data submitted by the training providers. Therefore, if a driver determines inaccurate information was submitted to the TPR, the driver must contact the provider to review, update, and resubmit records. The FMCSA cannot update records.

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).

Privacy Act requests concerning information in the TPR may be addressed to:

Nikki McDavid, Chief
Office of Commercial Drivers License
Federal Motor Carrier Safety Administration
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590
202-366-0831 https://tpr.fmcsa.dot.gov/Contact

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 TPR was developed and implemented under the authority of Section 32304 of the Moving Ahead for Progress in the 21st Century Act (MAP-21). Section 32304 of MAP-21 required the Agency to establish minimum training requirements for entry level drivers.

Training providers

FMCSA uses the contact information of training providers for purposes of being listed on the TPR and to allow entry-level drivers to locate training providers who are registered to provide entry-level driver training. FMCSA uses the training provider information to monitor the provider's competence and performance when providing training to driver-trainees and to uncover instances of fraud. FMCSA also uses the training providers' contact information to communicate with them regarding their information in the TPR.

Driver-trainee

The purpose of collecting, using, maintaining, or disseminating a driver-trainee's information is two-fold. First, it allows the desk agent at the respective SDLA to query the TPR and verify electronically that the applicant completed the applicable training prescribed in subpart F of part 380 when an individual applies for a CDL or endorsement. Second, these actions will provide FMCSA with data sources that it intends to use to assess the impact of ELDT on motor carrier safety and monitor the effectiveness of individual training providers.

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.

FMCSA proposes to maintain driver-trainee records for 60 years or until notified that the driver is deceased. This retention period is consistent with other CDL driver records maintained by FMCSA. The records schedule for the TPR records is currently being developed and will be submitted for approval by NARA. All records maintained in the system of records will be treated as permanent records until the schedule is approved by NARA.

FMCSA retains training certification information submitted to the TPR. FMCSA believes retention of this information is prudent in the event that data transmission to the SDLA is unsuccessful. Further, FMCSA intends to use the specific training information contained in the training certification information to assess the impact of ELDT on motor carrier safety and to monitor the effectiveness of individual training providers.

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.

FMCSA collects and uses data only to the extent necessary to meet its authorized safety mission. Disclosure of PII is limited to the purposes and uses specified in the Minimum Training Requirements for TPR.

Specifically, FMCSA publishes training provider information on the TPR for trainees so they can complete the applicable training prescribed in 49 CFR part 380. The trainee will not have access to any PII pertaining to training providers. Additionally, FMCSA intends to share driver training records, via the TPR, with the SDLAs so they can verify that a driver completed the applicable training prescribed in subpart F of part 380 when an individual applies for a CDL or endorsement.

If appropriate, additional information regarding the use and disclosure of information collected will be made in accordance with the U.S. Department of Transportation (DOT) Prefatory Statement of General Routine Uses published in the Federal Register on July 20, 2012 (77 FR 42796), under "Prefatory Statement of General Routine Uses" (available at www.transportation.gov/privacy).

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).

FMCSA ensures that the collection, use, and maintenance of PII for implementing the TPR is relevant to the purposes for which the data is to be used and, to the extent necessary for those purposes, it is accurate, complete, and up-to-date. The Agency has a variety of protocols in place to validate and verify that the information collected in the TPR is associated with the correct person to ensure the accuracy and reliability of the data collected. Those protocols include using a driver's CDL/CLP number and State of Issuance as a unique identifier. This data will be checked against the master CDL record of the State of Issuance.

The accuracy and reliability of the training provider information is self-certified by the training provider and reviewed and approved by FMCSA. Additional data checks are in place throughout the TPR system to ensure that data is of the highest quality. These include checks for completeness and validity for each data field type and required data element.

Although FMCSA has the responsibility to ensure that the data is transmitted appropriately, it relies on the accuracy of the data submitted by the training providers. Therefore, if a driver finds that inaccurate information was transmitted to the TPR and subsequently to the SDLA, the driver should contact the training provider that conducted his or her training, review the information that was submitted by the training provider, correct the information, and have the training provider resubmit the Training Certification Information to the TPR.

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.

PII is protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporates 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, and Recommended Security Controls for Federal Information Systems and Organizations, dated April 2013. The FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. All required authorizations (e.g., to operate, analysis) were established before the TPR was deployed. 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 TPR are safeguarded in accordance with applicable rules and policies, including all applicable DOT and FMCSA automated systems security and access policies. Strict controls are imposed on all DOT/FMCSA systems to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in the TPR 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 that are stored in the TPR will be protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the TPR is logged and monitored.

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

All FMCSA personnel and FMCSA contractors completes security and privacy awareness training and role-based training offered by DOT/FMCSA. This allows individuals with varying roles to understand and retain knowledge of how to properly and securely act in situations where they may use PII while performing their duties. No access is allowed to the TPR prior to receiving the necessary clearances and security and privacy training as required by DOT/FMCSA.

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 FMCSA employees and contractors accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA follows the Fair Information Practice Principles as best practices for the protection of PII associated with the implementation of the ELDT final rule. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees is 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/FMCSA Rules of Behavior. The FMCSA Information System Security Officer and FMCSA Privacy Officer conducts periodic security and privacy compliance reviews of the TPR consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Responsible Official

Nikki McDavid
Chief, CDL Division

Prepared by: Pam Gosier-Cox (FMCSA Privacy Officer)

Approval and Signature

Karyn Gorman
Acting Chief Privacy Officer