U.S. Department of Transportation

Federal Motor Carrier Safety Administration (FMCSA)

Privacy Impact Assessment
Pre-Employment Screening Program (PSP)

Responsible Official

Jeff Secrist
PSP System Manager
Federal Motor Carrier Safety Administration
jeff.secrist@dot.gov

Approval and Signature

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

Executive Summary

The Pre-Employment Screening Program (PSP) was implemented under the authority of Title 49 of the U.S. Code, Section 31150, titled "Safety performance history screening" as added by Section 4117(a) of the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU), Public Law 109-59, August 10, 2005. This statute requires the Department of Transportation's (DOT) Federal Motor Carrier Safety Administration (FMCSA) to make certain crash and inspection data about commercial motor vehicle (CMV) drivers, contained in the Motor Carrier Management Information System (MCMIS), available electronically to potential employers for conducting pre-employment screening. The PSP provides authorized motor carriers, industry service providers (ISP) and validated CMV drivers rapid electronic access to driver crash and inspection data for the purposes of conducting pre-employment screening. The program is managed and maintained by the FMCSA through its Service Provider. This Privacy Impact Assessment (PIA) is necessary to provide information regarding the program and the necessity to collect and share PII.

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.

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.

Overview of the Pre-Employment Screening Program (PSP)

The mission of FMCSA is to reduce crashes, injuries, and fatalities involving large trucks and buses (motor carriers). To carry out its safety mandate, FMCSA partners with stakeholders on efforts to reduce crashes involving motor carriers. Stakeholders include Federal, State, and local enforcement agencies; the motor carrier industry; safety groups; and organized labor. Since the first step towards reducing accidents is to understand them, FMCSA collects and maintains motor carrier and commercial driver safety data.

SAFETEA-LU requires FMCSA to make operator-applicant crash and inspection data available to potential employers. The PSP consolidates the processes required to implement the mandate to create an automated system for authorized access to crash and inspection data contained in Driver Information Resource (DIR) records. Through PSP, FMCSA provides authorized motor carriers, ISPs, and validated operator-applicants access to driver crash and inspection data for the purposes of conducting pre-employment screening.

PSP

The Pre-Employment Screening Program (PSP) provides motor carriers, industry service providers, and individual drivers access to commercial driver safety records from the Federal Motor Carrier Safety Administration's (FMCSA) Motor Carrier Management Information System (MCMIS). Records are available via the PSP website.

Driver Information Resource (DIR) Records

Each month, FMCSA provides the PSP service provider with an updated MCMIS data extract of driver crash data from the previous five (5) years and inspection data from the previous three (3) years. The MCMIS extract is used to create a driver profile known as the Driver Information Resource (DIR). The DIR includes the operator-applicants' name, driver's license number and issuing state, and the operator-applicants' driver/vehicle safety violations and inspection data. The service provider maintains the data in the PSP database and may not update the DIR under any circumstances. Individuals may request correction and amendment to their records through the DataQs system, as described below.

DataQs

DataQs is an online system for motor carriers, commercial drivers, Federal and State agencies, and the public to submit their concerns about publicly available Federal and State data contained in FMCSA data systems, including PSP.

When PSP data requires an update, an individual may submit a request for data review through DataQs. The request for data review is automatically sent to the appropriate office for resolution.

The change is then made to MCMIS and is updated in PSP during the next MCMIS snapshot that is provided to the service provider.

PSP Account Creation

For a motor carrier or ISP to access an individual operator-applicant's DIR, the motor carrier or ISP must first obtain a PSP account and be approved for PSP system use. To apply for a PSP account, the motor carrier or ISP must visit https://www.psp.fmcsa.dot.gov to access and complete the customer account holder agreement including provision of basic company information including contact address, phone number, and payment information for PSP monthly billing and agreeing to the terms and conditions of use. The ISP or motor carrier must also provide the first name, last name, and official email address of each user listed on the company's PSP account. Once completed, the account holder agreement is submitted electronically to the PSP service provider, who ensures the company is a valid entity with legitimate reasons for accessing PSP. If approved for PSP system access, the ISP or motor carrier users each receive a unique username and password from the DOT service provider. This username and password must be used every time the individual user accesses the PSP system.

Once an authorized ISP or motor carrier user accesses the PSP system, the authorized ISP or motor carrier user must certify, for each request, under penalty of perjury, that the request is for pre-employment purposes only and that they have disclosed to and obtained the written or electronic authorization of the operator-applicant (driver)

The PSP system also allows validated operator-applicants to access their own crash and inspection data upon written or electronic request. Upon receipt of an operator-applicant's request, the PSP system will validate the identity of the operator-applicant by using his or her full name, date of birth, driver's license number, issuing state and current address against a validation authority. The validation authority verifies that the submitted information matches available public data records held by the validation authority to ensure that an operator-applicant's DIR record is only released to that operator-applicant. At this point, PSP allows the operator-applicant to create a PSP username and password. The operator-applicant can access PSP via the unique username and password upon future visits to the PSP website. Once an operator-applicant has received his or her personal DIR, the operator-applicant will also receive an email providing access to revisit that DIR record for a period of five days from the time of purchase.

Neither DOT service provider, nor any subsequent PSP contractor, is authorized to provide data from the PSP system to any persons other than authorized ISP and motor carriers conducting pre-employment screening, and operator-applicants seeking a copy of their own safety data. The PSP system only allows operator-applicants to access their own data and authorized ISPS and motor carriers to access an individual operator-applicant's data if the authorized ISP or motor carrier certifies that the data is for pre-employment screening, and that it first disclosed to the operator-applicant that it is their intent to obtain the operator-applicant's PSP data, and then has obtained the operator-applicant's written authorization or electronic signature to obtain the data. A data request from any other person (e.g., a law firm) is treated as a Freedom of Information Act (FOIA)

request by FMCSA and processed accordingly. FMCSA has established an ongoing, random-selection audit process to monitor compliance with the disclosure and authorization obligation. The audit requirements and penalties process are part of the contract between FMCSA and the service provider. The process ensures that the account holder obtains a disclosure and authorization form, signed by the operator-applicant, prior to completing a PSP driver record inquiry in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) and 49 U.S.C. 31150. The service provider will penalize any account holder who fails to comply with the audit requirements. Based on the nature and frequency of these violations, the service provider may, on behalf of FMCSA, send a written warning, suspend, or terminate the account holder from the PSP. U.S. DOT can penalize the account holder with civil or criminal prosecution.

Personally Identifiable Information (PII) in PSP

Driver Profile (DIR)

CMV crash and inspection information. Data extracts from the FMCSA MCMIS containing the most recent five (5) years' crash data and the most recent three (3) years' inspection information for operator-applicants including:

- Operator-applicant's name (last, first)
- Operator-applicant's date of birth
- Operator-applicant's license number
- Operator-applicant's license issuing state

In accordance with 49 U.S.C. § 31150(a), the operator-applicant's safety information is extracted from MCMIS and made available for pre-employment screening comes from the following reports: CMV accident reports; inspection reports that contain no driver-related safety violations; and serious driver-related safety violation inspection reports.

PSP access transaction records.

The PSP database also includes records of access and transactions conducted by the PSP system when authorized individuals request a DIR on a prospective operator-applicant employee or when operator-applicants requested their personal DIR. These transaction records provide historical data of PSP usage by authorized requestors and facilitate accounting and compliance audits of the PSP by appropriate DOT/FMCSA officials.

In addition to DIR data, the access transaction records for account holders include the name of company requesting the DIR

In addition to DIR data, the access transaction records for operator-applicants include the individual's e-mail and physical address as well as phone number.

Fair Information Practice Principles (FIPPs) Analysis

The Fair Information Practice Principles (FIPPs) are rooted in the tenets of the Privacy Act and are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs are common across many privacy laws and provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis DOT conducts is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v.3i, which is sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council.

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 PII. Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Operator-applicants do not provide consent for their crash and inspection data to be included in the PSP system. Inclusion of their safety information in PSP is mandated by statute (49 U.S.C. 31150). The source of the information is the MCMIS database, which includes accident reports and field inspection reports. Operator-applicants may access their own DIR from PSP.

Although operator-applicants do not provide consent for their crash and inspection data that is included in the PSP system, operator-applicants must provide authorization for that information to be accessed from PSP by an ISP or a motor carrier for use in conducting pre-employment screening. The request, disclosure, and authorization process is as follows: Authorized ISPs and motor carriers must enter into an account holder agreement with DOT/FMCSA's PSP service provider to be "validated" to use PSP. No authorized ISP or motor carrier is allowed access to commercial driver safety data in PSP without first entering into an agreement with DOT's service provider. The account holder agreements contain the requirements of the PSP system. The account holder agreement may be viewed at www.psp.fmcsa.dot.gov.

Title 49 U.S.C. 31150(b)(2) requires that an authorized ISP or motor carrier must first disclose to operator-applicant that their PSP information will be used during the hiring process and the operator-applicant's written authorization must be obtained prior to releasing the crash and inspection data to that authorized ISP or motor carrier. An operator-applicant may provide either written or electronic authorization for the release of their crash and inspection data. To ensure the operator-applicant's authorization was obtained, the authorized ISP or motor carrier must certify for each request, under penalty of perjury, that the request is for pre-employment screening purposes only, and that authorization of the operator-applicant has been obtained. Records of operator-applicant consent are not maintained in PSP. The account holder agreement requires the authorized ISP or motor carrier to maintain all signed written consent forms for a minimum of three (3) years.

Authorized ISPs or motor carriers who use the PSP system are subject to monthly random audits by the DOT service provider and/or DOT/FMCSA.

The DOT service provider will be also routinely audited by DOT/FMCSA to ensure compliance with the contract and all applicable Federal laws and regulations, including the Privacy Act and the applicable sections of the Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 *et seq.* The FCRA, 15 U.S.C. Section 1681g(a), requires that the consumer reporting agency, upon request, disclose to the consumer the identification of each person that obtained a consumer report for employment purposes, during a 2-year period preceding the date on which the request was made and a record of inquiries received by the agency during a 1-year period preceding the request that identified the consumer in connection with a credit or insurance transaction that was not initiated by the consumer. Upon the request of the operator-applicant, FMCSA will identify each person who obtained a consumer report for employment purposes during a 2-year period preceding the date of the request. FMCSA will also release the "access transactions" record. Further, the DOT service provider provides all users with routine advisory statements that unauthorized use of the PSP system is strictly prohibited, and that misuse could be subject to criminal, civil or administrative sanctions under 18 U.S.C. § 1001 for any unauthorized use of the PSP system.

All other PII that PSP maintains is provided voluntarily by the operator-applicant. The only consequence of an operator-applicant not providing the information is the inability to use PSP to obtain the requested safety information. Records in PSP are maintained in accordance with DOT/FMCSA 007 - Pre-Employment Screening Program (PSP)[1]. The Department continues to evaluate the need for a separate PSP SORN as records in PSP are an extract of MCMIS and are covered by DOT/FMCSA 001 - Motor Carrier Management Information System (MCMIS)[2] Operator-applicants who do not wish to use PSP to obtain their safety information have the option to obtain it by submitting a Privacy Act request to FMCSA.

The PSP progressive web app (PWA) serves as an alternate method for authorized PSP users to access the PSP website on their phone or tablet. FMCSA does not require individuals to register or provide any PII as a condition of downloading the PSP PWA.

The publication of this PIA furthers demonstrates FMCSA's commitment to provide appropriate transparency into the Agency's operation of the Pre-Employment Screening Program.

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.

[1] See 77 FR 42548 , July 19, 2012.
[2] See 78 FR 59082, September 25, 2013.

PSP provides operator-applicants access to their own record. FMCSA provides redress through the DataQs system located at *https://dataqs.fmcsa.dot.gov* along with instructions to contact FMCSA if corrections to an operator-applicant's driver data are required. Operator-applicants may use DataQs to challenge safety information in their DIR. After a challenge has been properly submitted, DataQs automatically forwards the challenge to the appropriate office for resolution and allows the party that submitted the challenge to monitor its status. If the information is corrected, the change is then made in MCMIS, and the PSP system receives the change when the MCMIS data is refreshed. Under the Adjudicated Citations Policy, https://www.govinfo.gov/content/pkg/FR-2013-12-02/pdf/2013-28795.pdf, operator-applicants who have been found not guilty of a citation, or are convicted of a different citation, can submit the court documentation to DataQs and request FMCSA to correct the MCMIS record. If the MCMIS records are modified by the FMCSA, the updated record will be available in PSP upon the subsequent data refresh from MCMIS.

FMCSA is not authorized to correct state-level violation information. FMCSA directs any challenges to state-level violation information to the applicable state for processing and resolution. Additionally, FMCSA is not authorized to direct a state to change or alter MCMIS data for violations or inspections originating within that state.

Individuals wishing to correct MCMIS records shared with PSP may also use the procedures documented in DOT's Privacy Act regulations; see "Requests for Records" [49 CFR 10.31] and "Requests for Correction of Records" [49 CFR 10.41]. Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), operator-applicants seeking a copy of his or her driver record can make a request to the FMCSA FOIA office by sending a written request directly to:

Federal Motor Carrier Safety Administration
Attn: FOIA Team, MC-MMI 1200
New Jersey Avenue, SE
Washington, DC 20590

Statutory Authority and 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.

Title 49 of the U.S. Code, Section 31150, titled "Safety performance history screening" as added by Section 4117(a) of the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU), Public Law 109-59, August 10, 2005, requires FMCSA to make certain crash and inspection data contained in the Motor Carrier Management Information System (MCMIS) electronically available to potential employers for the purpose of conducting pre-employment screening. DOT/FMCSA uses PSP to make operator-applicant crash and inspection data readily accessible to authorized ISPs, motor carriers, and operator-applicants for pre-employment screening of prospective drivers. DOT/FMCSA employees and service provider personnel use the access

transaction records in PSP to administer external users' access requests and audit the PSP system and program and provide system support and maintenance.

Data Minimization and 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. Forms used for the purposes of collecting PII shall be authorized by the Office of Management and Budget (OMB)

The PSP system only maintains the data necessary to maintain access transaction records which verify the user requesting the information is a valid, trusted user. The data is collected only for the purposes outlined and maintained in accordance with the DOT/FMCSA 007 - Pre-Employment Screening Program, System of Records Notice (SORN). (March 8, 2010, 75 FR10557).

CMV crash and inspection records maintained in PSP are managed according to the General Records Schedule (GRS) 5.1, "Common Office Records" (https://www.archives.gov/files/records-mgmt/grs/grs05-1.pdf), item 020. These records are considered non-recordkeeping copies of electronic and each monthly MCMIS extract in PSP are be deleted after being superseded by a current MCMIS extract. If required for business use, they may be retained for a longer period. MCMIS is the authoritative source; therefore, it retains the recordkeeping version.

Pursuant to GRS 3.2, "Information Systems Security Records," item 031, concerning system access records, for systems requiring special accountability for access, PSP access transaction records are temporary records to be retained for six (6) years, then destroyed after passwords are altered or the user account is terminated, but a longer retention is authorized if required for business use.

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.

DOT/FMCSA uses PSP to make operator-applicant crash and inspection data readily accessible to authorized ISPs, motor carriers and operator-applicants for their pre-employment screening purposes. DOT/FMCSA employees and service provider personnel use the access transaction records in PSP to administer external users' access requests and audit the PSP system and program and provide system support and maintenance.

PSP information is not stored, maintained, used, or resold by the ISPs or motor carriers beyond pre-employment screening purposes. If an operator-applicant feels that their records have been requested without their consent or used for purposes other than pre-employment screening, inquires may be made via FMCSA_PSPHotline@dot.gov. DOT/FMCSA shares information from PSP with the following external users or systems:

- Authorized ISPs and motor carriers may access an operator-applicant's crash and inspection data in PSP with the operator-applicant's authorization.
- Validated operator-applicants may access their own crash and inspection data in PSP by completing the request process, verifying their identity, or authenticating with a username and password.
- To validate the identity of an operator-applicant seeking his or her own data, the DOT service provider submits information to a third-party validation authority (e.g. Lexis-Nexis).

Operator-applicants, authorized ISPs and motor carriers submit a DIR request to PSP by using the PSP website or the PSP PWA to submit operator-applicant-specific CMV information (full name, date of birth, driver's license number, and license issuing state). After receiving the request, the PSP system compares the individual's CMV information with operator-applicants in the MCMIS extract. When the PSP locates an individual's safety information in the MCMIS extract, the PSP system generates a DIR for delivery.

PSP delivers an operator-applicant's DIR to an authorized ISP or motor carrier at the completion of the website or PWA transaction. The authorized ISP or motor carrier user may view that record at no cost for five days from the time of purchase by logging in to the secure PSP website using a unique username and password. The PSP record is a PDF file and may be viewed, downloaded, or printed by an authorized user. Operator-applicants requesting their personal DIR also receive an email containing a hyperlink to the secure PSP website. The operator-applicant clicks the hyperlink, which returns them to the secure PSP website. Once there, the operator-applicant enters the unique user passcode furnished by the DOT service provider in the receipt email. When the operator-applicant's passcode and identifying information (date of birth, driver's license number, and license issuing state) are entered and accepted by PSP, the DIR may be viewed or printed by the requestor. Access to a purchased PSP record is available to an operator-applicant for five days from the time of purchase.

Data Quality & 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 PSP 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.

The DOT service provider has implemented the following measures to assure the accuracy of data presented in PSP records. Immediately following the monthly MCMIS extract upload to the PSP system, automated and manual reviews are conducted to ensure the data is accurate and complete. Additional steps taken to ensure that PSP system users receive accurate data include:

- Operator-applicants are given screen prompts to verify/confirm the accuracy of the information that he/she has entered. Once an operator-applicant request is submitted, the PSP system checks to determine if crash and/or inspection records exist in the most recent MCMIS data set available. That includes the exact information submitted by the operator-applicant. Only MCMIS crash and/or inspection records that contain all four data elements, (date of birth, last name, driver's license number(s) and license issuing state(s)) exactly matching the information typed by the operator-applicant, will be included on the PSP record returned to that operator-applicant. If no crash or inspection records are found that exactly match all four data elements, a response stating "no crash or inspection records found" is displayed.
- PSP requires ISP users and motor carriers to provide a unique username and password to access the secure information system and web interface. The username and password are validated against the DOT service provider customer account database to ensure the account is valid and active. Once authenticated, to complete a PSP record request, a motor carrier or ISP user must provide the same information required of operator-applicants to request records. The system institutes the same processes for identifying and retrieving records.

The monthly service provider extracts contain the most current crash and inspection data available in MCMIS. The DOT service provider is not permitted to alter or modify MCMIS data.

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.

All records in PSP are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Electronic files are stored in a database secured by passwords, encryption, firewalls, and operating systems to which only the authorized DOT service provider or DOT/FMCSA personnel with a "need to know" have access. Paper files are processed and immediately shredded securely. Paper files are only handled by the authorized DOT service provider and DOT/FMCSA personnel with a "need to know" requirement. All access to the electronic system and paper files is logged and monitored. The DOT service provider is subject to routine audits by DOT/FMCSA to ensure compliance with the Privacy Act, applicable sections of the Fair Credit Reporting Act, and other applicable Federal laws, regulations, and requirements. User access controls have been developed to ensure that the number of individuals with access to restricted information is kept to a minimum. Only users with a "need to know" are provided access. Audit controls are employed to ensure that PSP is used appropriately by authorized users and monitored for unauthorized usage. The data centers in which PSP operates are restricted access facilities.

For system access, PSP requires all authorized ISP and motor carrier users to be authenticated with a valid user identifier and password. User access to PSP is restricted within the system based upon the user's role as an authorized SIP, motor carrier, or validated operator-applicant. The unique identification and password must be used by a motor carrier or authorized ISP to access an operator-applicant's DIR. Further, an authorized ISP or motor carrier has signed a Monthly Account Holder Agreement with the DOT service provider and agreed to the PSP terms of use. To ensure that the account holder has disclosed their intent to view DIR data and is subsequently authorized by the operator-applicant to do so, the authorized ISP or motor carrier must certify under penalty of perjury, that the request is for pre-employment purposes only and that the authorization of the operator-applicant has been obtained. To ensure that the operator-applicant is seeking his or her own DIR record, additional authentication steps may be required to authenticate the identity of the operator-applicant.

The DOT service provider is required by the Securities and Exchange Commission to be compliant with the Sarbanes-Oxley Act (SOA) of 2002 [Public Law 107-204, 116 Stat. 745] and certified by an external auditor. The DOT service provider is also in compliance with the Information Technology General Control requirements included in Section 404 of the SOA.

The PSP system operates in accordance with the requirements of the Federal Information Security Management Act of 2002 (FISMA). Continuous monitoring activities are also performed annually to provide ongoing oversight of security controls and to detect misuse of information stored in PSP. In addition, PSP is subject to routine audits by DOT/FMCSA to ensure compliance with the Privacy Act of 1974; the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* dated March 2006; the NIST Special Publication (SP) 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* dated April 2013; all applicable sections of the Fair Credit Reporting Act; and all other applicable Federal laws and regulations.

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 will follow the Fair Information Practice Principles as best practices for the protection of PII associated with the Pre-Employment Screening Program. 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 DOT service provider will be given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance will be 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 will

conduct periodic security and privacy compliance reviews of the Pre-Employment Screening Program consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Responsible Official

Jeff Secrist
PSP System Manager
Federal Motor Carrier Safety Administration

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer