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
(202) 366-2039
Jeff.Secrist@dot.gov

Reviewing Official

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

PUBLICATION DATE

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, 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. To comply with the statute, FMCSA established the Pre-Employment Program (PSP) administered by a DOT Service Provider. The PSP provides authorized motor carriers and validated commercial motor vehicle (CMV) drivers (operator-applicants) 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 Federal Motor Carrier Safety Administration (FMCSA). This Privacy Impact Assessment (PIA) is necessary to provide information regarding the program and the necessity to collect 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 the Federal Motor Carrier Safety Administration (FMCSA), an Operating Administration within the U.S. Department of Transportation (DOT), is to reduce crashes, injuries, and fatalities involving large trucks and buses (motor carriers). To carry out its safety mandate, FMCSA partners with stakeholders—including Federal, State, and local enforcement agencies; the motor carrier industry; safety groups; and organized labor—on efforts to reduce crashes involving motor carriers. Since the first step towards reducing accidents is to understand them, FMCSA collects and maintains motor carrier and commercial driver safety data as well as a national inventory of motor carriers and shippers subject to Federal Motor Carrier Safety Regulations (FMCSR) and Hazardous Materials Regulations (HMR).

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, 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. The PSP Program embodies the required processes to implement the Congressional mandate to create an automated system for authorized access to Driver Information Resource (DIR) records. Through PSP FMCSA provides authorized industry service providers, motor carriers and authorized commercial motor vehicle (CMV) drivers (operator-applicants) rapid, electronic access to driver crash and inspection data for the purposes of conducting pre-employment screening.

Each month, FMCSA provides the PSP contractor with an updated MCMIS data extract containing driver crash data from the previous five (5) years and inspection data from the previous three (3) years. This MCMIS extract is used to create a driver profile known as the DIR. The DIR creates a driver profile using MCMIS crash data from the past five years and inspection data from the past three years. This profile shows PII data for the driver regardless of the employing carrier. The DIR also includes driver/vehicle safety violations and inspection data.

In order for an industry service provider or motor carrier to receive an individual operator-applicant's DIR, the industry service provider or motor carrier must first obtain a PSP account and be approved for PSP system use. To apply for a PSP account, the motor carrier or industry service provider must visit www.psp.fmcsa.dot.gov and download the customer account holder agreement. The motor carrier or industry service provider must complete the agreement, including providing basic company information including contact address, phone number, and payment information for PSP monthly billing. The company must agree to the terms and conditions of use. The motor carrier or industry service provider must also provide the first name, last name and email address of each user listed on the company's PSP account. Once completed, the account holder agreement is returned to the DOT service provider, who ensures the company is a valid entity with legitimate reasons for accessing PSP. If approved for PSP system use, the motor carrier or industry service provider users receive unique usernames and passwords from the DOT service provider that must be provided every time a user accesses the PSP system.

Once an authorized motor carrier or industry service provider user accesses the PSP system via username and password, the authorized industry service provider or motor carrier must certify, for each request, under penalty of perjury, that the request is for pre-employment purposes only and that written or electronic consent

of the operator-applicant has been obtained. Upon completion of certification, the DOT service provider will provide the individual operator-applicant data to the industry service provider or motor carrier via the secure PSP website or mobile application. The authorized industry service provider or motor carrier will access this individual's information by entering a unique identification and password, then providing information about the CMV driver to retrieve the DIR record from PSP. The motor carrier or industry service provider user has the option to view that record for a period of five days from the time of purchase.

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 requestor (operator-applicant) by using his or her full name, date of birth, driver license number, driver license 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 a CMV driver's DIR record is only released to that CMV driver. Once a CMV driver has received his or her personal DIR, the CMV driver 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 industry service providers, motor carriers conducting pre-employment screening, and commercial drivers seeking a copy of their own safety data. The PSP system only allows commercial drivers to access their own data and authorizedmotor carriers and industry service providers to access an individual operator-applicant's data if the authorized motor carrier or industry service provider certifies that the data is for pre-employment screening and that it has obtained the operator-applicant's written consent 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. DOT/FMCSA performs audits of the service provider to ensure that performance, privacy, and security objectives are met.

The contractor and FMCSA have established an ongoing, random-selection audit process to monitor compliance with the written consent obligation. The audit process to monitor compliance with the written consent obligation. The audit requirements and penalities process is incorporated by reference as part of the contract between FMCSA and the contractor. The purpose of the audit requirements and penalities process is to ensure that the account holder obtain a driver-signed consent form 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 contractor will penalize an account holder, who fails to comply with the audit requirements. Based on the nature and frequency of these violations, the contractor may send a written warning, suspend, or terminate the account holder from the PSP.

The electronic access to driver crash and inspection data is provided via the PSP website www.psp.fmcsa.dot.gov or through FMCSA's PSP mobile device application (FMCSA PSP)available through iTunes (www.itunes.apple.com). The mobile application is an Apple iOS (Apple Mobile Operating System) application downloadable to Apple iOS devices. Individuals downloading the iTunes application are required to fulfill Apple, Inc's (Apple) registration requirements prior to downloading the application. Apple's registration

requirements and privacy policy may be found at www.apple.com. FMCSA does not receive any of the registration information provided to Apple.

Pre-Employment Screening PII

The following PII is collected and maintained by FMCSA in support of the Pre-Employment Screening program.

1. *CMV crash and inspection information.* Data extract 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:

    - CMV driver name (last, first)
    - CMV driver date of birth
    - CMV driver license number
    - CMV driver license State

    In accordance with 49 U.S.C. § 31150(a), the CMV driver safety information 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.

2. *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 CMV driver employee or when CMV drivers 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. All access transaction records include information about the subject of the PSP record request that include the following PII data elements:*

    - CMV driver name (last, first, middle initial)
    - CMV driver date of birth
    - CMV driver license number
    - CMV driver license State

    Access transaction records also include information about the information requestor. In the case of an operator-applicant requesting his or her personal PSP record, the access transaction records will include the following PII data elements:

    - CMV driver name (last, first, middle initial)
    - CMV driver date of birth
    - CMV driver license number

- CMV driver license State
- CMV driver address.

In the case of a motor carrier or authorized industry service provider requesting the PSP record of an operator-applicant, the access transaction records will include the following PII data elements:

- PSP user unique system username
- PSP user unique system password

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.

CMV drivers do not provide consent for their crash and inspection data to be included in PSP; inclusion of their safety information in PSP is mandated by statute (49 U.S.C. 31150). Further, the source of the information is the MCMIS database, which includes accident reports and inspection reports (not from the drivers themselves). Although drivers do not provide consent for their crash and inspection data to be included in PSP, drivers must provide written consent for that information to be disclosed from PSP to an industry service provider or a motor carrier for use in conducting pre-employment screening. The request and consent process is as follows:

Authorized industry service providers and motor carriers must enter into an account holder agreement with DOT/FMCSA's PSP contractor to be "validated" to use PSP. No authorized industry service provider 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*, and clicking on the banner titled "PSP Enrollment."

Title 49 U.S.C. 31150(b)(2) requires that a driver's written consent be obtained prior to releasing the crash and inspection data to an authorized industry service provider or motor carrier. A driver may also provide electronic consent for the release of the driver's crash and inspection data. To ensure the driver's written consent was obtained, the authorized industry service provider or motor carrier must certify for each request, under penalty of perjury, that the request is for pre-employment screening purposes only and that written consent of the operator-applicant has been obtained. Additionally, the account holder agreement requires the authorized industry service provider or motor carrier to maintain all signed, written consent forms for a minimum of five (5) years. Authorized industry service providers or motor carriers who use the PSP system are subject to random audits by DOT Service Provider and/or DOT/FMCSA and DOT Service Provider will be 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 request of the driver, FMCSA will make available to the driver 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 the "access transactions" record. Further, DOT Service Provider provides users routine advisory statements advising that unauthorized use of the PSP system is strictly prohibited and that authorized industry service providers or motor carriers could be subject to criminal, civil or administrative sanctions under 18 U.S.C. § 1001 for misuse or abuse of the PSP system. The PSP maintains a privacy policy that complies with requirements of the E-Government Act of 2002.

All other PII that PSP collects (DIR profile information identifying the driver whose safety information is requested to be accessed) is provided voluntarily by the driver. The only consequence of not providing the information is inability to use PSP to obtain the requested safety information. Drivers who do not wish to obtain their safety information from PSP have the option to obtain it by submitting a Privacy Act request to FMCSA; authorized industry service providers or motor carriers have the option to submit a FOIA request for the information.

The PSP Mobile iOS Application serves as an alternative means of providing information available through the PSP website to the authorized users. FMCSA does not require individuals to register or provide any PII as a condition of downloading PSP iOS application. Individuals downloading the PSP iOS application must fulfill Apple's registration requirements prior to downloading the application. Apple does not provide FMCSA any PII of individuals who download the PSP iOS application from its site. Individuals who access the PSP website through the browser are subject to FMCSA's website privacy policy.

DOT has provided generalized notice to the public of its participation in the Pre-employment Screening Program through the DOT/FMCSA 007 - Pre-Employment Screening Program, System of Records Notice (SORN). (March 8, 2010, 75 FR10557). 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.

PSP does not directly provide redress, but it assists in directing redress requests to the source system (MCMIS). The PSP website provides a link to the FMCSA "DataQs" system located at *https://dataqs.fmcsa.dot.gov/login.asp* along with instructions to contact FMCSA if corrections to driver data are required. Drivers may use DataQs to challenge safety information in their driver profile (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. Individuals wishing to correct PSP records 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].

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 a particular State(s).

Under the provisions of the Privacy Act and FOIA, operator applicants seeking a copy of his or her driver record can make a request to 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

Stututory 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 CMV driver crash and inspection data readily accessible to authorized industry service providers, motor carriers and CMV drivers (external users) for their pre-employment screening

purposes. DOT/FMCSA employees and contractor 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)

CMV crash and inspection records: Pursuant to General Records Schedule (GRS) 20 ("Electronic Records," February 2008, see http://www.archives.gov/records-mgmt/ardor/grs20.html), which governs disposition of extract files, each monthly MCMIS extract in PSP is deleted approximately three (3) months after being superseded by a current MCMIS extract, unless needed longer for administrative, legal, audit, or other operational purposes.

Pursuant to GRS 24, "Information Technology Operations and Management Records, "Item 6, April 2010,[1]PSP access transaction records are retained for a period of five (5) years.

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 CMV driver crash and inspection data readily accessible to authorized industry service providers, motor carriers and CMV drivers (external users) for their pre-employment screening purposes. DOT/FMCSA employees and contractor 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 industry service providers or motor carriers beyond pre-employement screening purposes. If a CMV driver 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 users or systems outside DOT/FMCSA:

- Authorized industry service providers and motor carriers may access a driver's crash and inspection data in PSP with the operator-applicant's written consent or electronic signature.

[1]See, http://www.archives.gov/records-mgmt/grs/grs24.html

- Validated drivers may access their own crash and inspection data in PSP by completing the request process, verifying their identity.
- To validate the identity of a driver seeking his or her own data, DOT Service Provider submits information to a third-party validation authority (e.g. Lexis-Nexis).

The process by which a CMV driver, authorized industry service provider or motor carrier obtains a driver's DIR is as follows:

- CMV drivers, authorized industry service providers and motor carriers submit a DIR request to PSP by using the PSP website or the PSP mobile application to submit driver-specific CMV information (full name, date of birth, license number, and license State).
- After receiving the request, the PSP system compares the individual driver's CMV information with CMV drivers in the MCMIS extract. When the PSP locates an individual driver's safety information in the MCMIS extract, the PSP system generates an individual driver's DIR for delivery.
- PSP delivers a CMV driver's DIR to an authorized industry service provider or motor carrier onscreen at the completion of the website or mobile application transaction. The motor carrier, or authorized industry service provider 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 DIR may be viewed or printed by authorized users of the motor carrier or industry service provider requestor. Drivers requesting their personal DIR also receive an email containing a hyperlink to the secure PSP website. The CMV driver clicks the hyperlink, which returns the driver to the secure PSP website. Once there, the CMV driver enters the unique user passcode furnished by the DOT service provider to the driver in the receipt email. When the CMV driver's passcode and identifying information (date of birth, license number, and license State) are entered and accepted by PSP, the DIR may be viewed or printed by the requestor. No-cost access to a purchased PSP record is available to a CMV driver for five days from the time of purchase via the passcode and PSP website, after which time, the unique passcode expires.

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 hasimplemented the following strategies steps to assure the accuracy of data presented in PSP records made available to authorized requesters. Immediately following the monthly MCMIS extract upload to the PSP system automated and manual reviews of the PSP system are conducted to ensure the data was loaded accurately and completely. Additional steps are taken to ensure that PSP system users receive accurate data in PSP records.

- CMV drivers are given screen protmpts to verify/confirm the accuracy of the information that he/she has entered. Once a CMV driver request quest is submitted the PSP system checks to determine if

crash and/or inspection records exist in the most recent MCMIS data set avialble. that include the exact submitted by the driver. Only MCMIS crash and/or inspection records that contains all four data elements, (date of birth, last name, license number[s] and license state[s])exactly matching the information typed by the CMV driver, will be included on the PSP record returned to that driver. 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 returned.

- PSP requires motor carriers and ISP users to provide a unique username and password to access to 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, active, and that the username and password are accurate. Once authenticated, to complete a PSP record request, a motor carrier or ISP user must provide the same information required of CMV drivers for records requests and the system institutes the same proceses for identify and retrieving records.

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

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.

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 authorized DOT service provider or DOT/FMCSA personnel with a “need to know” have access. Paper files are stored in file cabinets in a locked file room to which only authorized DOT service provider and DOT/FMCSA personnel with a “need to know” have access. All access to the electronic system and paper files is logged and monitored. DOT service provider is subject to routine audits of the PSP program 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 in PSP is kept to a minimum and is restricted to only those with a “need to know.” Audit provisions are also included 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.

PSP requires all authorized motor carrier and industry service provider 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 industry service provider, motor carrier or validated operator-applicant. The unique identification and password must be used by a motor carrier or authorized industry service provider to access a CMV driver’s DIR. Further, an authorized industry service provider or motor carrier is an entity that has signed a Monthly Account Holder Agreement with DOT service provider and has agreed to the PSP terms of use. To ensure that

written or electronic consent of the operator-applicant has been obtained, the authorized industry service provider or motor carrier must certify for each request, under penalty of perjury, that the request is for pre-employment purposes only and that written consent of the operator-applicant has been obtained. To ensure that the CMV driver is seeking his or her individual DIR, additional authentication steps may be required to authenticate the identity of the driver.

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. DOT Service Provider is also in compliance with the Information Technology General Control requirements included in Section 404 of the SOA.

According to the Federal Information Processing Standards (FIPs) Publication 200, Minimum Security Requirements for Federal Information and Information Systems dated March 2006, the PSP system is authorized as a Moderate risk system. In accordance with the requirements of the Federal Information Security Management Act of 2002 (FISMA), a Security Authorization Process was completed for the PSP system and is authorized to operate for one year. 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. 3, *Recommended Security Controls for Federal Information Systems* dated December 2007; 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 Screeing 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 FMCSA 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 thePre-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

Original signed and on file with the DOT Privacy Office

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