



U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

Drug and Alcohol Clearinghouse

Responsible Official

David Yessen
Chief, Compliance Division
FMCSA Office of Enforcement and Compliance
(202) 366-1812
clearinghouse@dot.gov

Reviewing Official

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



Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an operating administration within the U.S. Department of Transportation (DOT). It's core mission to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, under the authority of the Moving Ahead for Progress in the 21st Century Act (MAP-21) (codified at 49 U.S.C. 31306a), FMCSA published a final rule titled, "Commercial Driver's License Drug and Alcohol Clearinghouse" (81 FR 87686). The rule amended the Federal Motor Carrier Safety Regulations to establish requirements for the Commercial Driver's License Drug and Alcohol Clearinghouse (Clearinghouse).

The Clearinghouse, a web-based system found at (<https://clearinghouse.fmcsa.dot.gov>), will provide FMCSA and employers of commercial motor vehicle (CMV) drivers with the necessary tools to identify drivers who are prohibited from operating CMVs due to DOT drug and alcohol program violations. The Clearinghouse will help ensure that such drivers receive the evaluation and treatment required by DOT regulation before being permitted to operate a CMV on public roads. Information maintained in the Clearinghouse will enable employers to identify drivers who commit a drug or alcohol program violation while working for one employer, but fail to subsequently inform another employer. Records of drug and alcohol program violations will remain in the Clearinghouse for five years, or until the driver has completed the return-to-duty process, whichever is later.

This Privacy Impact Assessment (PIA) is necessary to provide information regarding the Drug and Alcohol Clearinghouse 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.¹

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*

¹Office 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).

- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Clearinghouse is a database operated by FMCSA that will contain information about commercial driver's license (CDL) holders or commercial learner's permit (CLP) applicants' violations of FMCSA's drug and alcohol testing program. The Clearinghouse will provide FMCSA and employers the tools necessary to identify drivers who are prohibited from operating a CMV due to DOT drug and alcohol program violations and ensure that such drivers receive the required evaluation and treatment before operating a CMV on public roads. Specifically, information maintained in the Clearinghouse will enable employers to identify drivers who commit a drug or alcohol program violation while working for one employer, but fail to subsequently inform another employer (as required by current regulations).

To ensure that such drivers are identified, the following actions will be completed within the Clearinghouse:

- Employers will conduct pre-employment queries on prospective employees and if drug and alcohol violations are identified, those employees will be prohibited from performing safety-sensitive functions, until successful completion of the return-to-duty (RTD) process. Safety-sensitive functions are defined in 49 CFR § 382.107 as the time from when a driver begins to work or is required to be in readiness to work until the time he/she is relieved from work and all responsibility for performing work. Safety-sensitive functions include the time a driver is driving a CMV on public roads.
- Employers will query the Clearinghouse annually for each driver they currently employ, and if drug and alcohol violations are identified, those employees will be prohibited from performing safety-sensitive functions until successful completion of the RTD process;
- State Driver's License Agencies (SDLAs) will query the Clearinghouse before issuing, renewing, transferring, or upgrading a CLP or CDL;
- When requested by the National Transportation Safety Board (NTSB) as part of a crash investigation, FMCSA will provide NTSB information contained in the Clearinghouse concerning drivers who are involved in the crash under investigation.

Clearinghouse System Components

There are four main components of functionality within the Clearinghouse. These components are user registration, violation reporting, querying a driver record and requesting/providing consent to access a record. Each process is described below.

Registration:

All Clearinghouse users will be required to register for an account.

FMCSA and SDLA users will be required to log into the Clearinghouse via the FMCSA Portal. The Portal is a web-enabled system that is designed to authenticate users for various FMCSA IT Systems. User accounts are assigned access rights based on the roles and responsibilities of the individual user. For more information about the FMCSA

Portal, you may read the PIA for the FMCSA Portal, which is published on the DOT Privacy website (www.dot.gov/privacy).

Substance abuse professional (SAPs), medical review officers (MROs), and consortia/third-party administrators (C/TPAs) will be required to register for an account using login.gov. Login.gov is a General Services Administration (GSA) service developed as a single sign-on trusted identify platform for individuals to access government websites that require user authentication. After creating a login.gov account, users will single-sign on to the Clearinghouse, where they will register for specific rights based on the roles and responsibilities of the individual user. The PIA for login.gov is published by GSA and available for review at <https://login.gov/docs/Privacy-Impact-Assessment%209-18.pdf>.

SAPs, MROs, C/TPAs and employers may designate assistants to query, and/or report, within the Clearinghouse. Assistants will receive an invitation from their respective SAP, MRO, C/TPA or employer to register for a Clearinghouse account once an account and permissions have been established for them. The Assistants will not be able to register for a Clearinghouse account unless they receive an invitation. Once an assistant receives an invitation, he or she may login to the Clearinghouse using login.gov on behalf of their SAP, MRO, C/TPA, or employer.

Violation Reporting:

Once a user account is established, employers, MROs, SAPs, and C/TPAs and their assistants may use the Clearinghouse to report information related to violations of the drug and alcohol regulations (49 CFR parts 40 and 382) by current and prospective employees.

Table 1 below identifies when information must be reported by a required reporting entity to the Clearinghouse.

Reporting Entity	When information will be reported to the Clearinghouse
<p>Prospective/Current Employer</p>	<ul style="list-style-type: none"> • An alcohol confirmation test with a concentration of 0.04 or higher • Refusal to test (alcohol) as specified in 49 CFR 40.261 • Refusal to test (drug) not requiring a determination by the MRO as specified in 49 CFR 40.191 • Actual knowledge, as defined in 49 CFR 382.107, that a driver has used alcohol on duty, used alcohol within four hours of coming on duty, used alcohol prior to post-accident testing, or has used a controlled substance • Negative RTD test results (drug and alcohol testing, as applicable) • Completion of follow-up testing

Reporting Entity	When information will be reported to the Clearinghouse
Service Agent (C/TPA)	<ul style="list-style-type: none"> • An alcohol confirmation test with a concentration of 0.04 or higher • Refusal to test (alcohol) as specified in 49 CFR 40.261 • Refusal to test (drug) not requiring a determination by the MRO as specified in 49 CFR 40.191 • Actual knowledge, as defined in 49 CFR 382.107, that a driver has used alcohol on duty, used alcohol within four hours of coming on duty, used alcohol prior to post-accident testing, or has used a controlled substance • Negative RTD test results (drug and alcohol testing, as applicable) • Completion of follow-up testing
MRO	<ul style="list-style-type: none"> • Verified positive, adulterated, or substituted drug test result • Refusal to test (drug) requiring a determination by the MRO as specified in 49 CFR 40.191
SAP	<ul style="list-style-type: none"> • Identification of driver and the date of the initial assessment • Successful completion of treatment and/or education and the determination of eligibility for RTD testing

Table 1 - Reporting Entities and Circumstances

Query:

Employers or their designated C/TPAs are required to query the Clearinghouse for drug and alcohol program violations before hiring a prospective driver, and at least annually for all current drivers. A limited query will advise the employer or C/TPA if the Clearinghouse contains information about the driver; however, it does not result in the release of other information about the driver. However, when an employer initially queries the driver, a full query must be conducted. A full query will release detailed information contained in the Clearinghouse to the querying employer or C/TPA. An annual query may be conducted as either a limited query or a full query.

A full query will return the following information about the driver:

- Driver details
- Employer details
- Test details, including the type of test and violation details
- Information about who entered the test result

Consent Management:

Both limited and full queries require a driver's consent before any information can be released about that driver. A limited query requires a general consent. The general consent for the limited query may include consent to conduct limited queries that is effective for more than one year. General consent may be provided for an unlimited number of limited queries, such as for the duration of employment. The receipt of general consent for the limited query will

be handled outside of the Clearinghouse between the employer and employee. Once the employer obtains general consent, the employer will log into the Clearinghouse, select limited query, enter the driver's information, and submit the query. The Clearinghouse will return a message to the employer indicating whether the Clearinghouse contains drug or alcohol violation information for the queried driver.

If the limited query indicates that the Clearinghouse contains information on the driver, the employer or C/TPA must conduct a full query. The employer or C/TPA must obtain specific consent from the driver by logging into the Clearinghouse and requesting that the driver provide consent to release full query results (§ 382.703). When an employer requests a full query, the driver will receive notification of the request for specific consent via the preferred contact method indicated in their Clearinghouse account. To grant or decline specific consent, the driver will log into their Clearinghouse account. Once logged in, the driver will be able to either grant or decline consent to the requesting employer. If the driver provides consent, the employer will receive notification of the consent via email. The employer will then log into their account to view the detailed information for the queried driver.

If an employer is unable to obtain either general consent from a driver for a limited query, or specific consent for a full query, the employer must remove the driver from performing safety-sensitive functions, as described above.

Other system processes

In addition to violation reporting and querying, the Clearinghouse will be used by enforcement personnel at the roadside. Driver information from the Clearinghouse will be transmitted, whenever a driver's record is queried at the roadside using FMCSA's CDLIS Gateway and QueryCentral. Additionally, driver eligibility information will be transmitted to the National Law Enforcement Telecommunications System (Nlets) via the FMCSA Service Centers. This information will be used by roadside enforcement personnel and law enforcement officers to improve roadway safety by removing drivers who have tested positive for alcohol or drugs and have not completed their required return to duty (RTD) process. CDLIS Gateway, QueryCentral and Nlets will use a driver name, date of birth, CDL/CLP number and state of issuance to indicate a driver's eligibility in real-time when a driver is queried during roadside enforcement. Only a driver status of prohibited or not prohibited will be transferred to the roadside systems and specific violation information will not be transferred to these systems. PIA for all FMCSA systems may be found at <https://www.transportation.gov/privacy>

Personally Identifiable Information and the Drug and Alcohol Clearinghouse

The Clearinghouse maintains information about drivers who operate CMVs in interstate and intrastate commerce in the United States and are subject to the CDL requirements in 49 CFR part 382 or their Canadian and Mexican equivalents. In addition, the Clearinghouse will contain information on motor carrier employers, C/TPAs, SAPs, and MROs. FMCSA is responsible for ensuring appropriate protections governing the collection, use, sharing, storage, and retention of driver information under its control are properly implemented. As such, it is critical to ensure that positive drug and alcohol test results, test refusals, and employer reports of actual knowledge that a driver has violated any of the prohibitions under part 382 are accurately reported and are correctly attributed to the driver. Driver information maintained in the Clearinghouse includes, driver name, address, date of birth, CDL/CLP number, state of issuance, contact information, and login information.

There are several distinct user roles within the Clearinghouse. These roles are specific to: MROs, employers or C/TPAs and SAPs. Their roles are as follows:

- MROs are required to report to the Clearinghouse, within two business days, the following driver information for verified positive, adulterated or substituted test results and refusals to test (as provided in 49 CFR § 40.191):
 1. Reason for test (e.g., pre-employment, post-accident, random, reasonable suspicion, RTD, refusal to test, or follow-up);
 2. Federal Drug Testing Custody and Control Form specimen ID number;
 3. Collection site name and address;
 4. Driver's name, date of birth, and CDL/CLP number and state of issuance;
 5. Date of test;
 6. Date of the verified result;
 7. Specimen test result; and
 8. Employer information.
- Employers, or C/TPAs acting on behalf of an employer, including a driver who employs himself or herself, are required to report the following information to the Clearinghouse for: (1) an alcohol test result with an alcohol concentration of 0.04 or greater; (2) a negative RTD alcohol and/or controlled substances test result; (3) a refusal to take an alcohol test pursuant to 49 CFR 40.261; and (4) a refusal to provide a specimen for controlled substances testing pursuant to 49 CFR 40.191:
 1. Reason for the test;
 2. Driver's name, date of birth, and CDL/CLP number and state of issuance;
 3. Employer name, address, and USDOT number;
 4. Date of the test;
 5. Date of verified result;
 6. Test category
 7. Date the result was reported; and
 8. Test result.
- Additionally, employers are required to report each instance in which they have actual knowledge of any of the prohibitions a driver would be subject to in part 382. The information reported to the Clearinghouse must include the following information:
 1. Driver's name, date of birth, and CDL/CLP number and state of issuance;
 2. Employer name, address, and USDOT Number, if applicable;
 3. Date employer obtained actual knowledge of violation;
 4. Witnesses to the violation, if any, including contact information;
 5. Description of violation; and
 6. Evidence supporting each fact alleged in the description of the violation.
 - a. Evidence supporting each fact alleged may include, but is not limited to, affidavits, photographs, video or audio recordings, employee statements (other than admissions) correspondence, or other documentation.

- b. Employers reporting “failure to appear” drug or alcohol test refusals are required to provide contemporaneous documentation that the driver was notified to appear at the testing site and that the driver had not resigned or been terminated by the employer at the time the notification occurred.
- 49 CFR Part 40 Subpart O, *Substance Abuse Professionals and the Return-to-Duty Process*, requires SAPs to report the following information to the Clearinghouse:
 1. SAP name, address, and telephone numbers;
 2. Driver’s name, date of birth, and CDL/CLP number and state of issuance;
 3. Date of the initial SAP assessment; and
 4. Date when driver has successfully completed the education and /or treatment process and is eligible for RTD testing.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3², 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 Organizations³.

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.

FMCSA clearly discloses its policies and practices concerning all PII collected, maintained, used and disseminated pursuant to the implementation of all FMCSA rules. FMCSA provides notice to individuals several different ways. These include the publication of the Drug and Alcohol Clearinghouse Notice of Proposed Rulemaking and Final Rule⁴; the privacy policy on the FMCSA website (www.fmcsa.dot.gov); and the System of Records Notice (SORN) that will be published in the Federal Register and on the DOT Privacy Program website. The SORN will provide notice as to the conditions of disclosure and FMCSA’s routine uses for the information collected in the system. The SORN will also require that any dissemination of information maintained within the system be compatible with the purpose for which the information was originally collected. In addition, FMCSA will issue press releases, post information on the Clearinghouse website (<https://clearinghouse.fmsa.dot.gov>), send emails via a Clearinghouse listserv, provide

² <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

³ http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

⁴ <https://www.regulations.gov/docket?D=FMCSA-2011-0031>

periodic updates at industry outreach events, and post information related to the Clearinghouse on various social media outlets.

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

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.

FMCSA will ensure 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.

Drivers who register with the Clearinghouse will have access to review their information stored in the Clearinghouse. These drivers can view their record as often as they wish at no charge.

FMCSA will notify a driver when information about him or her has been entered or removed from the Clearinghouse, or has been revised. FMCSA will notify drivers by sending a letter via U.S. mail to the address on record with the SDLA that issued the CDL. A driver may also provide the Clearinghouse with an alternative means or address for notification. The driver will be alerted each time a change occurs to his or her record in the Clearinghouse.

Drivers have the right to review information about themselves in the Clearinghouse, except as restricted by law. Drivers may petition FMCSA to correct inaccurate information contained in the Clearinghouse. A correction may be requested if the alleged erroneous record is retained in the Clearinghouse.

Drivers are not able to challenge the accuracy or validity of the alcohol or controlled substance results under 49 CFR § 382.717(a)(1). However, exemptions are established under 49 CFR § 382.717(a)(2) to correct clerical errors, such as attributing drug or alcohol testing results to the wrong driver, reporting an incorrect driver name or CDL number, misidentifying the type of test performed (i.e., pre-employment screening versus random testing), and correcting other inaccuracies in the Clearinghouse. The petition can be submitted by the driver via the FMCSA DataQs system.

DataQs is a FMCSA electronic system for filing challenges, known as Requests for Data Review (RDR), to data that is maintained by FMCSA. To file a RDR, a driver or their authorized representative would need to create an account in DataQs and select "Add a Request". The RDR must include the petitioner name, address, phone number, CDL/CLP number, state of issuance, and detailed description and evidence supporting the inaccuracy. FMCSA will review the RDR in DataQs, and provide a notice of decision to remove, retain, or correct information in the Clearinghouse to the driver within 45 days of receipt. If data in the Clearinghouse is preventing a driver from performing safety-sensitive functions, they may request an expedited review within DataQs. FMCSA will notify the driver of its decision to any expedited requests within 14 days of receipt.

The DataQs procedures above can also be used by a driver to request that an employer's report of actual knowledge of a traffic citation for operating a CMV under the influence of drugs or alcohol be removed from the Clearinghouse if the citation did not result in a conviction. In addition, drivers can request that other reports of actual knowledge violations, as well as "failure to appear" test refusals, be removed from the Clearinghouse if they were not reported by the employer or C/TPA in accordance with 49 CFR § 382.705(b)(5). FMCSA will resolve petitions and notify drivers of its decisions within 45 days of receiving a complete petition. If the resolution of a petition will affect a driver's ability to perform safety-sensitive functions, he or she may request an expedited review. If FMCSA grants an expedited review, the Agency will inform the driver of its decision within 14 days of receiving a completed petition.

Under 49 CFR § 382.717(f) drivers may request that FMCSA conduct an administrative review if they believe that a decision resulting from the submitted petition was made in error. The driver will submit his or her request electronically, via the DataQs system (<https://dataqs.fmcsa.dot.gov>) or in writing to the Associate Administrator for Enforcement (MC-E), Federal Motor Carrier Safety Administration, 1200 New Jersey Avenue SE, Washington, DC 20590. The request must explain the error that the driver believes FMCSA has made and provide information and/or documents to support the driver's argument. FMCSA will complete its administrative review no later than 30 days after receiving the driver's request for review and this will constitute final Agency action.

Independent of the provisions provided in the final rule, 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/Privacy Act program may be found on the DOT website. Privacy Act requests concerning information in the Clearinghouse may be addressed to:

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

In addition, under 49 CFR part 10, subpart E, individuals may request that their records be corrected by submitting a written request detailing the correction requested and the reasons the correction should be made. If FMCSA does not make the requested correction to the individual's record, the individual may file a concise statement of disagreement setting forth the reason for disagreement with the Agency's refusal to amend the record. 49 CFR part 10, subpart F explains the individual's right to appeal the Agency's initial determination not to amend the record.

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.

FMCSA will use the information reported to the Clearinghouse to combat the problem of CDL or CLP holders testing positive for drugs or alcohol, or committing other drug or alcohol violations, and then continuing to operate CMVs without completing the required evaluation and treatment.

The reporting of positive test results and other drug and alcohol program violations will supplement the database employers must check to determine whether current or prospective employees are prohibited from operating CMVs under the DOT drug and alcohol testing program.

All violation information collected within the Clearinghouse will be used to address the problem of a driver who previously tested positive being able to obtain work without prospective employers knowing of and acting on that test information. This could occur if a driver does not inform employers about a previous positive test result. This could also occur if a new driver tests positive for drugs or alcohol during a pre-employment test, waits for the drugs to leave his/her system, then takes and passes another pre-employment test, and the results of the second test are used by the hiring employer without having any knowledge of the previous, failed test.

Additionally, FMCSA enforcement users will use the Clearinghouse data to ensure that employers are following the query procedures specified in 49 CFR § 382.701 and that MROs, SAPs, C/TPAs and employers are following the reporting procedures of 49 CFR § 382.705.

To determine whether the driver is qualified to operate a CMV, SDLAs may query the Clearinghouse any time a driver seeks to obtain, renew, transfer, or upgrade a CDL.

NTSB accident investigators will be provided information contained in the Clearinghouse to determine if CDL holders involved in crashes under investigation had an existing drug or alcohol program violation when the crash occurred.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

As required by 49 CFR §382.705, information reported to the Clearinghouse must include the driver's name, date of birth, CDL/CLP number and state of Issuance. This information will only be used to identify and verify a driver within the Clearinghouse. Social security numbers will not be collected or stored within the Clearinghouse.

As required by 49 U.S.C. 31306a(g)(6)(B), information will remain in the Clearinghouse indefinitely if a driver fails to complete the RTD process. Information will be removed from the Clearinghouse if: (1) the SAP reports that the driver has successfully completed the prescribed education and/or treatment as required by 49 CFR § 40.305 and is eligible for RTD testing; (2) the employer or C/TPA reports that the driver has received negative RTD test results; (3) the driver's present employer or C/TPA acting on the employer's behalf reports that the driver has successfully completed all follow-up tests as prescribed in the SAP's report in accordance with 49 CFR §§40.307, 40.309, and 40.311; and (4) five years have passed since the date of the violation determination. Clearinghouse records may be removed earlier than five years under procedures pertaining to the correction or removal of inaccurate information established in the final rule and in 49 CFR part 10.

Required Clearinghouse documents, including drug and alcohol violation evidence and driver notification letters will be stored for the Clearinghouse in the FMCSA Cloud Environment. The Cloud Environment is FedRAMP compliant, commercial cloud environment and infrastructure (Amazon Webservices [AWS] Cloud). All documents that are stored will be encrypted.

Records will be retained and disposed in accordance with the records control schedule DAA-0557-2016-0001, "Commercial Driver's License Drug and Alcohol Clearinghouse" approved by the National Archive and Records

Administration (NARA) on December 22, 2016. Records in the Clearinghouse will be closed after 5 years and destroyed when 7 years old or destroyed 7 years after cutoff.

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 may use the information in the Clearinghouse to identify and take enforcement action against employers, MROs, SAPs, C/TPAs, and CDL/CLP drivers that are not in compliance with the Agency's regulations. In addition, driver data may be used to remove a driver with unresolved drug or alcohol program violations from performing safety-sensitive functions. State Enforcement personnel will have access to a driver's eligibility via other FMCSA systems, such as Query Central and the CDLIS Gateway.

FMCSA will provide the NTSB information about a driver's drug and alcohol violations contained in the Clearinghouse when that driver is involved in a crash under investigation by the NTSB.

SDLAs may use information contained in the Clearinghouse to determine whether an individual is eligible to operate a CMV by querying the Clearinghouse any time a CDL/CLP is issued, renewed, transferred, or upgraded. SDLAs are prohibited from making any other use of the information or further disseminating the information obtained by conducting driver-specific queries.

Employers may only use information obtained from the Clearinghouse to determine whether a driver is prohibited from operating a CMV or from other safety-sensitive activities. Employers are strictly prohibited from making any other use of the information or further disseminating the information. Unauthorized use of Clearinghouse data is subject to civil and criminal penalties.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

The Agency will have a variety of protocols in place to validate and verify that the information collected in the Clearinghouse 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 at the State of Issuance. Additional data checks will be in place throughout the Clearinghouse 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. The petition and administrative review processes allows drivers to request that FMCSA review and correct inaccurately reported information.

FMCSA ensures that the PII collected, used, and maintained in the Clearinghouse is relevant to the purposes for which it is to be used, is accurate, complete, and up-to-date. FMCSA also ensures that proper access controls, information input restrictions, data validity checks, error handling mechanisms, information output handling and audit logs, and accountability protocols, are in place.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

PII is protected by reasonable security safeguards against loss or unauthorized access, destruction, misuse, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under FISMA and the information security standards issued by National Institute of Standards and Technology (NIST), including Federal Information Processing Standards (FIPS) Publication 200 and NIST SP 800-53 Revision.4, Recommended Privacy and Security Controls for Federal Information Systems. FMCSA has a comprehensive information security and privacy program that contains administrative, technical, and physical safeguards that are appropriate for the protection of data. These safeguards are designed to achieve the following objectives:

- Ensure the security 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

The Clearinghouse will maintain 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 list, and other security methods, FMCSA will prevent unauthorized access to data stored in its Clearinghouse. These controls will meet federally mandated information assurance and privacy requirements.

No one will be permitted to access the Clearinghouse without a valid username and password. The Clearinghouse will have controls to limit access based on FMCSA-approved user roles and responsibilities, and need to know. No person or entity will be able to share, distribute, publish, or otherwise release any information in the Clearinghouse except as specifically authorized by law. Reporting inaccurate or misleading information to the Clearinghouse will be expressly prohibited and subject to civil and criminal penalties. The Clearinghouse personnel, including government personnel and contractors, are required to take annual security awareness and privacy training offered by FMCSA as well as role-specific training. This will allow individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use PII in the course of performing their duties.

The Clearinghouse will undergo the security assessment and authorization process under NIST Special Publication 800-53, Revision 4 prior to attaining full operational status.

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 will follow the Fair Information Practice Principles for the protection of PII associated with the implementation of the Clearinghouse. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records.

As with any collection of PII, there is a risk of misuse of the information. To mitigate the risk, FMCSA will restrict access to the Clearinghouse by establishing strict registration procedures for drivers, employers and their C/TPAs, MROs and SAPs. All Clearinghouse users will be required to provide names, addresses, telephone numbers, and other information necessary to validate identity. Employers will be required to submit the names of all persons authorized to access the Clearinghouse on behalf of the employer. Employers will be required to designate authorized C/TPAs and drivers will be required to identify authorized SAPs before a C/TPA or SAP can be granted access to enter information into the Clearinghouse on behalf of that employer or driver. MROs and SAPs will be required to provide evidence that they meet DOT qualifications and training requirements. Employers and C/TPAs will be required to update annually the names of the people they authorize to access the Clearinghouse on their behalf. This information will be subject to specific registration protocol for MROs and SAPs. The initial registration term will be five years unless FMCSA has revoked or canceled a user's registration. FMCSA will also cancel registrations that are inactive for two years. FMCSA prohibits anyone from knowingly reporting false or inaccurate information. FMCSA will have the right to revoke the registration of anyone who fails to comply with any of the prescribed rights and restrictions on accessing the Clearinghouse, which will include (but not be limited to) submission of inaccurate information, misuse or misappropriation of access rights, misuse of protected information, and failure to maintain the requisite qualifications, certifications, or training requirements included in 49 CFR Part 40. Anyone violating these provisions will be subject to the civil and criminal penalties included in 49 CFR Part 382.507, as well as any other applicable penalties.

In addition, FMCSA is responsible for identifying, training, and holding agency personnel accountable for adhering to agency privacy and security policies and regulations. FMCSA has incorporated its Best Practices for Protection of PII in the design and implementation process for the Clearinghouse. The FMCSA Security Officer and FMCSA Privacy Officer will conduct regular periodic security and privacy compliance reviews of the L&I consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

David Yessen"
Chief, Compliance Division
FMCSA Office of Enforcement and Compliance
(202) 366-1812
clearinghouse@dot.gov

Reviewing Official

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