U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)
Automated Compliance Review System (ACRS)

Responsible Official

Michael Gordon
ESL Team Leader
304-549-2651
michael.gordon2@dot.gov

Reviewing Official

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

7/9/2014

X Claire W. Barrett

Claire W. Barrett
DOT Chief Privacy & Information Asset Officer
Signed by: CLAIRE W BARRETT

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an Operating Administration within the U.S. Department of Transportation (DOT) with a core mission to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, FMCSA created the Automated Compliance Review System (ACRS) web-based system to track State implementation of Commercial Drivers License (CDL) regulations as part of State compliance reviews performed by FMCSA. This program involves database support, user training, coordination of multiple State and Federal agencies to ensure understanding and cooperation between parties involved in the compliance assurance process, and management of various user roles. This Privacy Impact Assessment (PIA) is necessary to provide information regarding the ARCS 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*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

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

Introduction & System Overview

FMCSA has engaged in over ten years of comprehensive compliance reviews of State Commercial Driver's License (CDL) programs, and has conducted reviews in coordination with a review of each State (approximately every three and one-half years). To date, FMCSA has reviewed each State at least three times and the results from compliance reviews are documented as compliance findings. When not in compliance, States must submit a Corrective Action Plan (CAP) designed to mitigate compliance issues including specific actions that the State plans to take to correct the finding and

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

their estimated completion date. Once one or more actions are completed, the State must submit an updated it's CAP. In some instances, FMCSA determines that a finding purportedly addressed by a State actually remains outstanding because the State has not taken sufficient corrective action to mitigate the deficiency. FMCSA identifies these as repeat findings.

Through the implementation of the Automated Compliance Review System (ACRS), FMCSA has automated the document exchange aspects of the compliance review and CAP submission process including the submission of findings, CAPs, and CAP updates. ACRS aids in the completion of CDL compliance reviews and facilitates the tracking of data associated with these reviews. ACRS does not perform the review in itself, but it is used to keep track of the large number of documents provided by the State to complete a review and the items after action reports.

Personally Identifiable Information (PII) and ACRS

As part of the State CDL compliance reviews, FMCSA may collect and store Commercial Driver's License Information System (CDLIS) driver records in ACRS. FMCSA uses the CDLIS driver records evidence a problem that State needs to correct. The predominant PII stored in the CDLIS driver records stored in ACRS is the CDL driver's State driver license number. The driver license numbers are embedded into the reports that FMCSA develops to summarize the compliance findings in each State. The driver license numbers are used by the licensing States to locate specific record within their State's CDLIS database, so that the State may be able to resolve their compliance findings.

In order to assert that a mitigation activity included in the State's CAP in response to a specific FMCSA finding is addressed the States must provide evidence that a corrective action has been taken and the finding resolved. States provide the necessary evidence of completion to FMCSA by uploading the documents directly to ACRS. ACRS contains a document repository that is only accessible to authorized FMCSA and State users.

FMCSA does not limit the document formats or content uploaded by the States as evidence of completion for a corrective action stored in ACRS for review by FMCSA. As a result the files maintained in ACRS may contain information specific to individual drivers that that the State user wishes to submit to FMCSA to support the State compliance activities, therefore these records may contain individual;

- Name.
- Date of birth.
- Social Security Number (SSN).
- Gender.
- Height.
- Weight.
- Eye color.
- Driver license number.
- License State-of-Record.

Fair Information Practice Principles (FIPPs) Analysis

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

Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2]*, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*[3]*.*

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

FMCSA informs the public that their PII is collected, stored, and used by ACRS through this Privacy Impact Assessment published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, and all uses of the PII collected, stored, and transmitted through ACRS.

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.

All PII collected by FMCSA and stored in ACRS is provided by State-operated CDLIS databases and is used as an example of State compliance review findings. Therefore, the CDLIS State-of-Record is the authoritative source for CDLIS driver records stored in ACRS. Since these State-operated CDLIS databases are the authoritative sources for all driver information contained in the records, ACRS does not provide CDL drivers with any additional notice, options for consent, or options to seek redress. Any CDL drivers who wish to contest the accuracy of their information that is located in a State-operated CDLIS databases must direct their redress requests to the applicable State Driver Licensing Agency (SDLA). FMSCA does not place limitations on the types or sources of documents that States provide as evidence of findings remediation and the States may include records other than those maintained in the State's CDLIS database. States are responsible for providing appropriate notice, as required, to individuals that their information will be included in the submission to FMCSA.

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.

As part of its compliance review process, FMCSA may store some examples of CDLIS driver records from that specific State in ARCS. These CDLIS driver records serve as an example to demonstrate a problem identified by FMCSA in the compliance review and one that State needs to correct. ACRS stores driver license numbers and other minimal PII within the example CDLIS driver records to enable licensing States to locate specific records within their CDLIS database. These driver license numbers are not used by ACRS to retrieve CDLIS driver records. In addition, ACRS contains a

[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

document repository which allows State users to upload and submit to FMCSA supporting documentation to illustrate that corrective action has been taken in response to a compliance review finding. Primarily all documentation within ACRS represents the findings and information of a State's level of compliance with FMCSA regulations.

The documents uploaded to ACRS remain a part of that State's record within ACRS to illustrate the State's compliance history. For example, if during a future compliance review FMCSA identified a finding for a violation that was previously cited during a review, the documentation contained in ACRS would demonstrate that the State has repeatedly committed specific violations over a period of time. ACRS does not collect any data from the public, nor is the ACRS accessible by members of the public. In addition, ACRS does not provide the ability to use data, such as the driver license number, to retrieve the driver's information. Instead, ACRS provides an authorized FMCSA or state user with the ability to query whether a State has findings, and to provide details about the specific findings for each State so that the State may then locate the specific driver record in their own State database. All PII contained in the system is maintained to either provide an example of a specific finding identified in the compliance review or demonstrate that a State took corrective action in response to a finding.

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.

FMCSA stores the examples of CDLIS driver records within ACRS from specific States which had problems identified by FMCSA during a State CDL compliance review and to identify the specific issues that State needs to correct. ACRS stores minimal PII elements within the example CDLIS driver records which enable licensing States to locate the specific records serving as examples of the issues found during the compliance review within their CDLIS database. Once these example driver records are identified, the State can begin to take corrective action to resolve the finding.

Authorized State and FMCSA users also have the ability to upload documents, which can contain PII, to ACRS in support of State compliance efforts. These supporting documents stored in the ACRS document repository can potentially contain any information that the users wishes to submit to FMCSA. FMCSA does not specify what documents or information the individual States must provide to demonstrate that corrective action has been taken in response to a compliance review finding.

The records within ACRS, which contain summary reports on field activities, are retained for 5 years in accordance with the provisions of the U.S. National Archives and Records Administration (NARA) SF 115: NI-557-05-6, Item 7B,[4] unless needed longer for administrative, legal, audit, or other operational purposes.

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.

[4] NARA SF 115: NI-557-05-6, Item 7B. Commercial Driver's License (CDL) Program Files: Contains copies of summary reports on field activities and field reviews conducted by headquarters on the regional CDL program. Part 7B: Other files. Disposition: Temporary. Cutoff at end of each fiscal year. Determine medium of recording keeping copy. a) If electronic: Destroy paper documents after the information has been converted into an electronic medium, backed up, and verified. Delete electronic files 5 years after cutoff. b) If paper: Destroy paper documents 5 years after cutoff.

PII in ACRS is only used as an example of problems identified during State CDL compliance reviews and documents the findings of non-compliance by a State. ACRS does not provide the ability for authorized users to use the data stored in the system, such as the driver license number, to retrieve a specific driver's information. Instead, ACRS provides an authorized FMCSA or state user with the ability to query whether a State has non-compliance findings, and to provide details about these specific findings for each State. This then allows the individual States to locate the specific driver record in their own State database and take corrective action.

Authorized State users have the ability to upload documents to a document repository within ACRS in support their State compliance efforts. These supporting documents stored in the ACRS document repository can potentially contain any information that the State users want to submit to FMCSA to provide evidence of their activities to correct compliance review findings. FMCSA does not specify the types documents or information that the individual States must submit to demonstrate that corrective action has been taken in response to a compliance review finding. Therefore, any PII contained in the uploaded documents is up to the State's discretion.

The information contained within ACRS is not shared with any other Agency or Organization. No other FMCSA programs use the information contained within ACRS.

Data Quality and Integrity

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

All information received from the individual States and stored in ACRS is provided by State-operated CDLIS databases. This information has been identified as examples of driver records that support the specific State CDL compliance review findings.

The individual State will upload all information that it considers necessary to present its case stating that the finding cited in the compliance review by FMCSA has been corrected into the ACRS document repository. FMCSA relies upon the State to ensure that the uploaded information is correct.

All the data uploaded in the ACRS system can only be viewed by authorized personnel from that specific State, specifically designated FMCSA Division personnel overseeing that State, the regional Service Center person in charge of Compliance Reviews for that region, and a select group of Headquarters personnel who have been granted access to the system.

ACRS relies on the States for the data quality and integrity of the CDLIS records data as the information is collected, owned, and maintained by the individual States. FMCSA can only ensure the confidentiality and integrity of PII contained in ACRS once the information has already been received from the individual States. FMCSA is not permitted to modify CDLIS driver records retrieved from the States' CDLIS databases.

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.

The FMCSA Office of Information Technology has provided guidance to assist the contractor in protecting the confidentiality, integrity, and availability of information, including PII, stored in or retrieved by ACRS.

The data center in which ACRS operates is a restricted access facility. Physical access to the ACRS system is limited to appropriate personnel through applicable physical security requirements of the agency. FMCSA and contract support personnel with physical access have all undergone and passed DOT background checks.

All information stored in or retrieved by ACRS is protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Electronic files are stored in databases secured by passwords, firewalls, and operating systems to which only authorized personnel with a "need to know" have access. The ACRS login screen warns users of penalties for unauthorized access, and all access to information retrieved by ACRS is logged and monitored.

User access controls have been developed to ensure that the number of individuals with access to restricted information stored in or retrieved by ACRS is kept to a minimum and is limited to only those individuals with a "need to know." Access to information in ACRS, including PII, is strictly limited to only the specified authorized personnel and is determined by permission levels. ACRS employs role-based access controls and privileges based on whether the user is a State or Local official or an FMCSA employee. User accounts are assigned access rights based on the roles and responsibilities of the individual user. Individuals requesting access to ACRS must submit some personal information (e.g., name, contact information, and other related information) to FMCSA as part of the authorization process. Such authorized users may add / delete data commensurate with their requirements.

Users are required to authenticate with a valid user identifier and password in order to gain access to ACRS. This strategy improves data confidentiality and integrity. These access controls were developed in accordance with Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* dated March 2006 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems* dated April 2013. Regular monitoring activities are also performed annually to provide ongoing oversight of security controls and to detect misuse of information stored in or retrieved by ACRS.

All ACRS users are made aware of the FMCSA Rules of Behavior (ROB) for IT Systems prior to being assigned a user identifier and password and prior to being allowed access to ACRS. The general public does not have access to ACRS.

After a review of the security and privacy controls, ACRS was initially authorized to operate (ATO) in February 2013 and was issued a new ATO in June 2014..

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FMCSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA will follow the Fair Information Principles as best practices for the protection of information associated with the ACRS system. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records.

Federal and contract employees will be given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance will be provided in the form of mandatory annual Security and privacy awareness training

as well as Acceptable Rules of Behavior. The FMCSA Security Officer and FMCSA Privacy Officer will conduct regular periodic security and privacy compliance reviews of ACRS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Audit provisions are also included to ensure that ACRS is used appropriately by authorized users and monitored for unauthorized usage. All FMCSA information systems are governed by the FMCSA Rules of Behavior (ROB) for IT Systems. The FMCSA ROB for IT Systems must be read, understood, and signed by each user prior to being authorized to access FMCSA information systems, including ACRS. FMCSA contractors involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to access ACRS.

Responsible Official

Michael W. Gordon
ESL Team Leader
304-549-2651
Michael.gordon2@dot.gov

Reviewing Official

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