U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)
Analysis and Information Online (A&I) System

Responsible Official

Bill Bannister, FMCSA-MC-RRA
Chief of the Anaylsis Division
(202) 385-2388
William.Bannister@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) with a core mission to reduce commercial motor vehicle-related crashes and fatalities. To further this mission, FMCSA created the Analysis & Information Online (A&I) web-based system (https://ai.fmcsa.dot.gov/default.aspx) to facilitate compliance reviews and roadside inspections by providing quick and efficient access to descriptive statistics and analyses regarding commercial vehicle, driver, and carrier safety information. This system is used by Federal, State, and local law enforcement personnel, as well as the motor carrier industry, insurance companies, and the general public.

This Privacy Impact Assessment (PIA) update is necessary to addresses risks associated with migrating the A&I system to the FMCSA Cloud Enviornment.

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.

[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 M-03-22 dated September 26, 2003).

Introduction & System Overview

A&I Online is a web-based system that supports FMCSA's Compliance, Safety and Accountability (CSA) initiative and its operational model test; provides the basis of the statistical analysis that is performed; and provides safety history and ratings for commercial motor vehicles, commercial drivers, and carrier safety information. A&I is designed to facilitate compliance reviews and roadside inspections by providing Federal, state, and local enforcement officials with quick and efficient access to descriptive statistics and analyses of motor carrier, CMV, and CMV driver safety information. Descriptive statistics and analyses provided by A&I may also be used by Federal, state, and local enforcement officials to initiate enforcement actions against motor carriers and CMV drivers that fail to comply with Federal Motor Carrier Safety Regulations and Hazardous Materials Regulations. A&I also provides a centralized location for accessing the safety records of both intrastate and interstate motor carriers, as well as CMV drivers, in order to facilitate the administration of various FMCSA programs.

A&I contains the data related to these processes and allows all authorized users access to that data in the performance of their duties. A&I does not directly collect information, including PII. The data contained in A&I is received in a monthly snapshot from the Motor Carrier Management Information System (MCMIS).

A&I processes and provides safety information that has PII as follows:

- **Safety Measurement System:** The Safety Measurement System (SMS) is an automated system that quantifies the on-road safety performance of motor carriers so that FMCSA can identify unsafe carriers, prioritize them for intervention, and monitor if a motor carrier's safety and compliance problem is improving. The SMS results can be an important factor in determining the safety fitness of carriers. The SMS identifies the carriers demonstrating the worst safety performance so that they can be considered for an "Unfit" safety determination. The SMS will continuously monitor on-road performance to assess whether an entity's safety performance has improved enough for it to exit the Intervention Process, or if further intervention is warranted. Findings from the SMS will allow the evaluated carriers to view an assessment of their weaknesses in various safety areas. In turn, this information will empower motor carriers and other stakeholders involved with the motor carrier industry to make safety-based business decisions.
- **Driver Safety Measurement System:** The Driver Safety Measurement System (DSMS) is a tool for FMCSA and state partners to evaluate a driver's performance. Law enforcement officials use the DSMS results to examine the safety performance of individual CMV drivers when conducting CSA program investigations. Currently, the DSMS results are being used strictly as an investigative tool for law enforcement and are not available to carriers, drivers, or the public. However, the raw safety information from roadside inspections and crashes that feeds the DSMS is compiled by the same system that provides CMV driver-based data to FMCSA's Driver Pre-Employment Screening Program (PSP). This program allows motor carriers to access driver inspection and crash records electronically as a part of the hiring process.
- **FMCSA Tools:** This module includes information resources available on A&I Online that are only accessible to FMCSA employees and State partners via user id and password authentication. This module has a sub module:
    - **Driver Information Resource:** The Driver Information Resource (DIR) provides a secure web-based lookup capability that allows FMCSA and State enforcement personnel to view a driver's crash and inspection history by driver name or commercial driver license number. A driver's crash and/or violation data will be displayed if the driver had an inspection within 3 years or a crash within 5 years. All crash and inspection events that meet these criteria will be displayed along with the motor carrier

for whom they were operating. The system also allows FMCSA and State enforcement to search by U.S. DOT number or carrier name to obtain a list of all drivers affiliated with the specified carrier that had an inspection within 3 years or a crash within 5 years. The DIR module receives a monthly snapshot of inspection and crash data from MCMIS. The data includes PII such as driver name, Driver's License Number, date of birth and age.

Personally Identifiable Information (PII) and A&I

A&I Online uses PII to provide motor carrier safety information, including statistical and analytical resources for FMCSA and State enforcement personnel. A&I contains the data for the performance of compliance reviews and inspections on motor carrier operations, inspections of commercial motor vehicles, and other data elements which may result in enforcement actions being taken against a motor carrier for failure to adhere to motor carrier and laws and regulations. It is used by Federal, State, and local law enforcement personnel as well as the motor carrier industry, insurance companies, and the general public.

A&I does not directly collect information. A&I receives a snapshot of data, some of which is PII, from the MCMIS database each month. The uploaded data is not altered in anyway once it enters the system. Information in A&I is an exact copy of the MCMIS database and is refreshed every month with new information from MCMIS. MCMIS is a central repository for the efficient sharing of information about CMV drivers and motor carriers and is frequently accessed by Federal, State, foreign and local government agencies.

A&I contains both PII and non-PII on commerical motor vehicles (CMV) drivers. The information fields contained in A&I are as follows:

- Last, first, and middle names
- Date of dirth
- Driver’s License Number
- Issuing state of CMV drivers and co-drivers license
- Employer Identification Numbers
- Social Security Number (for owner-operators who use their SSN as their EIN)
- Home Address (for sole proprietor-drivers, owner-operators)
- Home telephone number (for sole proprietor-drivers, owner-operators)
- Age
- Employment history

A&I receives a monthly snapshot from the MCMIS which includes Social Security Numbers (SSNs) and/or Employer Identification Numbers (EINs). The SSNs and EINs are collected when the motor carrier or individual registers for a USDOT Number or Operating Authority and is verified during the safety audit or compliance review process. The SSN is collected from sole proprietors who do not have an EIN number. FMCSA encourages sole proprietors to obtain an EIN and to provide it when applying for their USDOT number registration. The collection of an SSN will be solely used for identification purposes.

MCMIS is the authoritative source of PII in A&I. The MCMIS system obtains PII from roadside CMV and CMV driver inspections and crash reports submitted by state and local law enforcement agencies and from investigations performed by State and Federal investigators. State officials and FMCSA field offices forward safety information to

MCMIS after it has been compiled and processed locally. Motor carrier information is obtained by company officers that have completed the Motor Carrier Identification Report. Company officers must sign to the accuracy of the information reported.

Move to the FMCSA Cloud Environment

As part of the Administration's ongoing plans and actions to modernize and enhance IT tools that support FMCSA mission processes for registration, inspection, compliance monitoring, and enforcement, a number of core FMCSA enterprise applications, including A&I, have been migrated from a private in-house DOT hosting environment and general support services infrastructure to a commercial cloud environment and infrastructure (the Amazon Webservices [AWS] Cloud,) known as the FMCSA Cloud Environment.

Initial transition into the FMCSA Cloud Environment followed a lift-and-shift migration approach to replicate the existing application and infrastructure hosting environment directly onto the infrastructure-as-a service (IaaS) platform provided by the AWS Cloud. In following this technical migration approach, FMCSA enterprise applications were not redesigned or modified to accommodate the physical transition to the new AWS Cloud IaaS platform or environment. The risks associated with this migration are discussed in the Security section of this PIA.

For more information on the FMCSA Cloud Environment please refer the the FMCSA Cloud Environment PIA, available on the DOT Privacy Office website at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

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.

A&I does not collect PII directly from individuals. A&I only stores a copy of PII that has been collected through MCMIS for statistical analysis of historical data. It is not the authoritative source for the PII data. The A&I website has a link to the DOT Privacy Policy, which contains all the protection and advisories required by the E-Government Act of 2002. The Privacy Policy describes DOT information practices related to the online collection and the use of PII.

As MCMIS is the primary source for information stored in A&I, notice is also provided to individuals through the Privacy Act System of Records Notice (SORN) for MCMIS (DOT/FMCSA 001 - Motor Carrier Management Information System (MCMIS) - 78 FR 59082 - September 25, 2013). The MCMIS SORN is available to the public on the DOT Privacy Office website and from the Federal Register (http://www.gpo.gov/fdsys/pkg/FR-2013-09-25/pdf/2013-23131.pdf). The

MCMIS web interface also provides notice, via the DOT Privacy Policy, to all individuals who enter their own PII into MCMIS.

FMCSA informs the public that their PII is stored and used by A&I through this Privacy Impact Assessment, published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to store and use the PII, and all uses of the PII stored and transmitted through A&I. The A&I PIA is available at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

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.

A&I does not collect PII directly from individuals. A&I receives a snapshot of data, some of which is PII, from the MCMIS database on a monthly basis. The uploaded data is not altered in any way once it enters the system. MCMIS is the authoritative source of PII in A&I. The MCMIS system obtains information, including PII, from roadside CMV and CMV driver inspections and crash reports submitted by State and local law enforcement agencies, and from investigations performed by State and Federal investigators. A motor carrier can log into the MCMIS website at any time using their PIN number to update the information that is stored, including any PII data. Motor carriers also currently have the option of filling out an updated MCS-150 form and mailing to FMCSA-HQ for data entry.

A&I does not directly provide redress. FMCSA provides redress for A&I through the DataQs systems and A&I includes a link to the DataQs system. The DataQs system (https://dataqs.fmcsa.dot.gov/login.asp) is an electronic means for filing concerns about Federal and state data released to the public by FMCSA. Individuals can use DataQs to challenge information included in their records. Motor carriers, state agencies, and FMCSA offices can use DataQs to challenge information concerning crashes, inspections, compliance reviews, safety audits, enforcement actions, vehicle registrations, operating authorities, insurance policies, and consumer complaints stored in any FMCSA system, including A&I. After a challenge has been 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 as a result of the challenge, the change will be made in MCMIS. A&I will receive the changed information through the monthly snapshot from MCMIS.

DataQs cannot be used to challenge safety ratings or civil actions managed under 49 CFR 385.15 (Administrative Review) or 49 CFR 385.17 (Change to Safety Rating Based upon Corrective Actions). Any challenges to information provided by state agencies must be resolved by the appropriate state agency.

Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), individuals may request searches of A&I or MCMIS to determine if any records have been added that may pertain to them. This is accomplished 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

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.

A&I uses PII collected by other FMCSA information systems to provide quick and efficient access to descriptive statistics and analyses regarding commercial vehicle, driver, and carrier safety information. A&I contains the data for the performance of compliance reviews and inspections on motor carrier operations, inspections of commercial motor vehicles, and other data elements which may result in enforcement actions being taken against a motor carrier for failure to adhere to motor carrier and laws and regulations. It is used by Federal, State, and local law enforcement personnel as well as the motor carrier industry, insurance companies, and the general public.

The purpose of the system is to facilitate compliance reviews and roadside inspections by providing Federal, State, and local enforcement officials with quick and efficient access to descriptive statistics and analyses of motor carrier, CMV, and CMV driver safety information. This information may be used to initiate enforcement actions against motor carriers and CMV drivers that fail to comply with FMCSRs and HMRs. A&I also provides a centralized location for accessing the safety records of intrastate and interstate motor carriers and of CMV drivers in order to facilitate the administration of various FMCSA programs.

The following A&I modules are part of A&I online used by users for the purposes described here:

- **Driver Information Resource (DIR)**—DIR creates a CMV driver profile using monthly snapshots of data from FMCSA's Motor Carrier Management Information System (MCMIS) crash records from the past five years and inspection records from the past three years. This profile includes CMV driver PII regardless of the employing motor carrier. DIR also maintains CMV and CMV driver safety violations and inspection records.
- **Driver Safety Measurement System (DSMS)**—DSMS utilizes MCMIS information in support of the Compliance, Safety, and Accountability (CSA) initiative and its operational test model. DSMS uses information from CMV and CMV driver safety violations and crash and inspection records to classify CMV driver safety performance into seven categories.
- **Safety Measurement System (SMS)**—SMS utilizes MCMIS information to assess motor carrier regulatory compliance and safety performance and to support the CSA initiative. SMS evaluates the safety of motor carriers using CMV and CMV driver safety violations and crash and inspection records.

Access to the DIR module is restricted to authorized FMCSA employees and contractors, and state agencies participating in the Motor Carrier Safety Assistance Program (MCSAP).

Access to the DSMS module is restricted to authorized FMCSA enforcement personnel, FMCSA Headquarters (HQ) support staff, and MCSAP state agencies.

Access to the SMS module is restricted to authorized FMCSA enforcement personnel, FMCSA HQ support staff, Federal and local law enforcement officials, MCSAP state agencies, FMCSA-grantee law enforcement agencies, and motor carriers. In addition, the general public can use the SMS module to view motor carrier registration and safety information.

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

FMCSA only uses and retains data that are relevant and necessary for the purpose of A&I. A&I Online receives a monthly snapshot from the MCMIS which includes PII determined to be necessary for A&I system functions. A&I retains and disposes of information in accordance with the approved records retention schedule as required by the U.S. National Archives and Records Administration (NARA).

The A&I master files are logged and regularly backed up. The master backup tape is retained in a secure offsite storage facility and then destroyed in accordance with applicable NARA retention schedule N1-557-05-07 Item #1. The master backup tape is designated for deletion under this retention schedule when 5 years old, when no longer needed, or when information is superseded or becomes obsolete, whichever is sooner.

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.

The FMCSA minimizes its data collection to that necessary to meet the authorized business purpose and mission of the Agency. A&I information is used to provide quick and efficient access to descriptive statistics and analyses regarding commercial vehicle, driver, and carrier safety information.

The A&I system does not share PII data with any other systems. A&I Online is not the authoritative source for the PII data, PII data is collected from other FMCSA systems for statistical analysis of historical data. It is used by Federal and State enforcement personnel, as well as the motor carrier industry, insurance companies, and the general public.

The following groups have access to A&I:

- CMV Drivers, Motor Carriers, and General Public—Have access to view statistical analysis and generalized reports only. No authentication is required.
- Motor Carriers—Can log into A&I to view all of their own safety and registration data.
- FMCSA and State Enforcement Users—Authorized FMCSA users have full access to all of the data to review and monitor the applications. A User ID and password is required to access the system.
- System Administrators and Developers—Federal contractors (System administrators and developers) have full access to the A&I Online to perform their assigned roles and responsibilities (development and maintenance of the system).

The A&I website can be accessed via the single sign-on (SSO) FMCSA Portal. Access through the FMCSA Portal is restricted to FMCSA enforcement personnel, FMCSA Headquarters (HQ) staff, MCSAP state lead agencies and Motor Carriers.

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 FMCSA ensures that the use and maintenance of information collected for operating the A&I system is relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, that it is accurate, complete, and up-to-date.

A&I does not collect PII directly from individuals. A&I only stores and disemminates PII that has already been collected through the Motor Carrier Mangement Information System (MCMIS). MCMIS is the authoritative source for the data stored in A&I.

The MCMIS system provides internal data edit checks on all data submitted to MCMIS. FMCSA data entry contractors have a verification process to ensure that accurate information is entered in MCMIS. MCMIS requires motor carriers to submit a Motor Carrier Identification Report (MCS-150) to obtain a USDOT Number, and uses internal validation functionality to ensure that all required data fields have been completed on the MCS-150.

FMCSA data entry contractors have a four-step verification process to ensure that accurate information is entered in MCMIS regardless of whether the forms are received via fax or mail. When an application is received, the first step is to review the application to ensure that all required data elements are present. The next step is to verify that the data is correct. Step three is to enter the information into MCMIS. The last step is verification and final approval that the data entered into MCMIS matches the data on the form.

Individuals who provide PII through FMCSA forms to request MCMIS reports provide that PII directly and are responsible for its accuracy. FMCSA staff reviewing and approving submitted forms check for completeness on required fields and verify requirements when there is a question of whether a requestor has the right to a report containing PII.

Individuals who submit PII to obtain direct access to MCMIS must submit this information directly to FMCSA. These individuals may contact their approving supervisor for any corrections to submitted information.

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, usage, modification, or disclosure. These safeguards incorporate standards and practices required for Federal information systems under the Federal Information System Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006; and NIST Special Publication (SP) 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013. FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII.

- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII.
- Protect against unauthorized access to or use of PII.

Records in the A&I system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in the A&I system is limited to those individuals on a need-to-know basis for the performance of their official duties, and who have appropriate clearances and permissions. All records in the A&I system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the A&I system is logged and monitored.

Logical access controls restrict users of the A&I. These controls are guided by the principles of least privilege and need-to-know. Role-based user accounts are created with specific job functions allowing only authorized accesses, which are necessary to accomplish assigned tasks in accordance with compelling operational needs and business functions of the A&I system. Any changes to user roles require approval of the System Manager. User accounts are assigned access rights based on the roles and responsibilities of the individual user. Individuals requesting access to A&I 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 and/or delete data commensurate with their requirements.

Users are required to authenticate with a valid user identifier and password in order to gain access to A&I. 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 A&I.

A&I Online requires FMCSA and State enforcement personnel to be authenticated with a valid user name and password, except for users of the public web application. The general public access is unrestricted via http://ai.fmcsa.dot.gov.

The A&I maintains an auditing function that tracks all user activities in relation to data, including access and modification. FMCSA prevents unauthorized access to data stored in the A&I system through technical controls including firewalls, intrusion detection, encryption, access control list, and other security methods. These controls meet Federally mandated information assurance and privacy requirements.

FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training, and role-based training offered by DOT/FMCSA. This training allows 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. No access will be allowed to the A&I prior to receiving the necessary clearances and security and privacy training as required by DOT/FMCSA. All users at the Federal and state level 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 A&I.

A security authorization is performed every year to ensure that A&I meets FMCSA and Federal security requirements. A&I also undergoes an additional security authorization whenever a major change occurs to the system. A&I is assessed in accordance with the Office of Management and Budget (OMB) Circular A-130 Appendix III, Security of Federal

Automated Information Resources and the DOT Certification and Accreditation Guidance. A&I is approved through the Security Authorization Process under the National Institute of Standards and Technology (NIST). As of the date of publication of this PIA, the A&I was last authorized on June 23, 2014.

Security Assurances Inherited from the AWS Cloud

Use of the AWS Cloud allows FMCSA to re-use and leverage a FedRAMP-compliant cloud system environment and approved Federal cloud service provider (CSP). The AWS FedRAMP compliant environment consists of the AWS Cloud network and AWS internal data center facilities, servers, network equipment, and host software systems that are all under reasonable control by AWS. The AWS Cloud environment and service facilities are restricted to US personnel, and all AWS Cloud community customers are restricted to US government entities from Federal, state or local government organizations.

The AWS environment had been evaluated and tested by FedRAMP-approved, independent third-party assessment organizations (3PAOs). The AWS is designed to meet NIST SP 800-53 minimum security and privacy control baselines for information and/or Federal information systems' risk up to Moderate impact levels. As confirmed through audit, the AWS addresses recent requirements established by NIST SP 800-171 for Federal agencies to protect the confidentiality of controlled unclassified information in non-federal information systems and organizations. AWS provides FIPS Pub 140-2-compliant services to protect data-at-rest with AES-256-based encryption and validated hardware to secure connections to the AWS.

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 A&I 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 the A&I 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 A&I 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 A&I. FMCSA contractors involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to access A&I.

Responsible Official

Bill Bannister, FMCSA-MC-RRA
A&I Business Owner & Chief of the Anaylsis Division
(202) 385-2388
William.Bannister@dot.gov

Approval

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