U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

Licensing and Insurance (L&I) System

Responsible Official

Betsy Benkowski

Office of Registration and Safety Information

202-366-5387

Betsy.Benkowski@dot.gov

Reviewing Official

Claire W. Barrett

Chief Privacy & Information Asset Officer

Office of the Chief Information Officer

privacy@dot.gov

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=CLAIRE W BARRETT
Date: 2017.03.21 12:32:11 -04'00'

Executive Summary

The Federal Motor Carrier Safety Administration's (FMCSA) Licensing and Insurance (L&I) system was implemented under the authority of 49 U.S.C., Section 13902, titled "Registration of Motor Carriers," and 49 CFR 365 "Rules Governing Applications for Operating Authority." In addition, 49 U.S.C., Section 31138, titled "Minimum Financial Responsibility for Transporting Passengers," and Section 31139, titled "Minimum Financial Responsibility for Transporting Property" prescribe the minimum levels of financial responsibility required to be maintained by commercial motor carriers of property and passengers operating motor vehicles in interstate, foreign, or intrastate commerce. L&I is a web-based application that contains licensing and insurance information on active and inactive interstate motor carriers, freight forwarders, and property brokers from the United States, Canada, and Mexico that have applied for interstate commerce authority.

L&I facilitates the application process for interstate commerce authority; filing of insurance and process agent (BOC-3) coverage; serving of Operating Authorities and issuance of certificates, permits, and licenses; revocation of Operating Authorities for lack of insurance. It also facilitates the process for applying for interstate commerce authority, protesting the granting of an authority, and reinstating Operating Authorities.

This Privacy Impact Assessment (PIA) update is necessary to address risks associated with migrating the L&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*

[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).

- *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 mission of the Federal Motor Carrier Safety Administration (FMCSA), an Operating Administration within the U.S. Department of Transportation (DOT), is to reduce crashes, injuries, and fatalities involving large trucks and buses (motor carriers). To carry out its safety mandate, FMCSA partners with stakeholders—including federal, state, and local enforcement agencies; the motor carrier industry; safety groups; and organized labor—on efforts to reduce crashes involving motor carriers. Since the first step towards reducing accidents is to understand them, FMCSA collects and maintains motor carrier and commercial driver safety data as well as a national inventory of motor carriers and shippers subject to Federal Motor Carrier Safety Regulations (FMCSR) and Hazardous Materials Regulations (HMR).

Commercial motor carriers that transport, or arrange for the transport of, passengers or federally regulated commodities in interstate commerce are required by FMCSA to have interstate operating authority in accordance with 49 U.S.C., Section 13902, titled "Registration of Motor Carriers," and 49 CFR 365, "Rules Governing Applications for Operating Authority." In addition, 49 U.S.C., Section 31138, titled "Minimum Financial Responsibility for Transporting Passengers," and Section 31139, titled "Minimum Financial Responsibility for Transporting Property" prescribes the minimum levels of financial responsibility required to be maintained by commercial motor carriers of property and passengers that operate motor vehicles in interstate, foreign, or intrastate commerce. FMCSA has established the Licensing and Insurance (L&I) system as the authoritative source for commercial motor carrier licensing and insurance information. L&I contains the licensing and insurance information for more than 330,000 commercial motor carriers, freight forwarders, and property brokers from the United States, Canada, and Mexico that have applied for interstate commerce authority.

The L&I operating environment includes the following elements:

- L&I Internal Intranet-Based Subsystem—The L&I internal Intranet-based subsystem is accessed at http://li.fmcsa.dot.gov/ and allows authorized FMCSA personnel to enter licensing and insurance information. The L&I internal Intranet-based subsystem also supports interactive entry of OP-1(MX) and OP-2 applications by border offices, entry of transferred information, selection of USDOT Numbers from the Motor Carrier Management Information System (MCMIS), retrieval of insurance and licensing letters, retrieval of name changes from the FMCSA registration system, and access to information concerning the status of commercial motor carriers, hazardous material shippers, and companies with blanket designations for BOC-3 forms.
- L&I Public Internet-Based Subsystem—The L&I public Internet-based subsystem is limited to specific functions. This subsystem is accessed at http://li-public.fmcsa.dot.gov/ and allows commercial motor carriers, freight forwarders, and property brokers to submit and track the status of applications for operating authority. Insurance companies, surety companies, and financial institutions use this subsystem to file certificates and cancellations, view their last transmissions, and print their confirmation, acceptance, and reject reports. The L&I public Internet-based subsystem is also used to designate process agents (BOC-3) for commercial motor carriers, freight forwarders, and property brokers. Anyone may query this subsystem to determine if a commercial motor carrier, freight forwarder, or property broker is active or inactive and if they have satisfied the requirements for registration. All information displayed in this query is public information that is available under the Freedom of Information Act (FOIA).

- L&I Operating Authority Management (OAM) Portlet—The L&I OAM Portlet allows authorized federal and state users to perform the same functions as the L&I internal Intranet-based subsystem and is accessed via FMCSA Portal.

For-hire motor carriers, brokers, and freight forwarders must obtain operating authority from FMCSA by registering in the L&I System or submitting a hard copy of the appropriate Interstate Operating Authority (OP) series form.[2] L&I facilitates the application process for interstate commerce authority; filing of insurance and process agent (BOC-3) coverage; serving of Operating Authorities and issuance of certificates, permits, and licenses for motor carriers, freight forwarders, and property brokers. Commercial motor carriers, freight forwarders, and property brokers can use L&I to submit their licensing and insurance information electronically and to pay the application processing fee with a credit card via Pay.gov.[3]

Applicants for operating authority must pay an application fee by credit card or electronic check before FMCSA will process the application. Credit card payments are collected by the L&I System and passed to the government electronic bill payment service (Pay.gov) for processing. The credit card information is stored in an encrypted form in FMCSA's system only during the processing of the operating authority application fee. Except for the last four digits of the card number, the credit card number is deleted after the operating authority transaction payment process has been completed. The last four digits of the credit card are stored to provide FMCSA a means to trace un-authorized or suspicious transactions.

Applicants can also apply for operating authority through the US Mail by completing the OP series form and submitting a credit card number, personal check or money order. Check payments are sent to Bank of America (BoA) for processing. Once the payment is processed, BoA sends a copy of the canceled check or money order to the FAA, then the FAA forwards a copy of the cancelled check or money order to FMCSA as receipt that the payment was processed. Credit card payments through the US Mail are processed by FMCSA employees through the Pay.gov electronic bill payment service.

The L&I website allows commercial motor carriers, freight forwarders, and property brokers to access their own information with a valid USDOT Number, Freight Forwarder Number, or Docket Number, in addition to a Personal Identification Number (PIN). Only authorized FMCSA personnel with a specific "need to know" can access non-public information concerning commercial motor carriers, freight forwarders, and property brokers.

Personally Identifiable Information (PII) and L&I

The L&I system collects business information from sole proprietors, commercial motor carriers, freight forwarders, and property brokers as part of the registration process:

1. Owner-operator licensing and insurance information—L&I authorizes commercial motor carriers, freight forwarders, and property brokers from the United States, Canada, and Mexico for interstate commerce. The authorization process requires entities to submit the following information to L&I:
    - Business name
    - Address

[2] OP series form may be found here - http://www.fmcsa.dot.gov/documents/forms/r-l/op-1-instructions-and-form.pdf (Last accessed, July 7, 2014.)

[3] The pay.gov system is managed by the US Department of Treasury's Financial Management Service. The PIA for pay.gov may be found at http://www.fms.treas.gov/pia/paygov_pia%20.pdf. (Last accessed July 7, 2014)

- Phone number
- Representative who can respond to inquiries.
  - Name
  - Title, Position, or Relation to Applicant
  - Address
  - Phone Number

2. Financial transactions. Some owner-operators may submit hardcopy L&I application forms to FMCSA along with one of the following forms of fee payment:
   - Owner-operator/Spouse bank name and account number (from cancelled check)
   - Owner-operator/Spouse credit card number
3. Court issued documents:
   - L&I uses state issued corporate documents and court issued decisions (i.e. wills, divorce certificates, court rulings of ownership) of owner-operators to facilitate name changes and ownership changes.

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 L&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.

The L&I website contains a link to the DOT Privacy Policy at the bottom of the webpage, which applies to online information practices only. The online registration form (https://www.fmcsa.dot.gov/registration/getting-started) identifies the data fields that are required and those that are voluntary. In addition, the DOT Privacy Policy states that "by providing personally identifiable information, you are granting us consent to use this personally identifiable information for the primary purpose for which you are providing it. Additionally, we will ask for you to grant us consent before using your voluntarily provided information for any secondary purposes, other than those required under the law."

The hardcopy L&I registration form states that "all responses to this collection of information are mandatory, and will be provided confidentiality to the extent allowed by the Freedom of Information Act (FOIA)."

To use the Insurance Filing option, a user name and password is required. To obtain a user name and password, you must register with the FMCSA as an electronic filer and you must be a representative of an insurance company, surety company or financial institution. Registered electronic filers may file certificates and cancellations, view their last transmissions, and print their confirmation, acceptance, and reject reports.

FMCSA informs the public that their PII is stored and used by L&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 L&I. The L&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.

FMCSA provides redress for individuals whose records may be maintained in the L&I system through its Motor Carrier Information Management system (MCMIS) and DataQs system. The L&I website provides a link to the DataQs system (https://dataqs.fmcsa.dot.gov/login.asp) along with instructions to contact FMCSA if corrections to L&I records are required. DataQs allows a filer to challenge data maintained by FMCSA on, among other things, USDOT Number registration, operating authority registration, and insurance matters. Through this system, any registration-related data concerns are automatically forwarded to the appropriate FMCSA office for resolution. If the information is corrected as a result of the challenge, the change will be made in MCMIS. L&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 FOIA, individuals may request searches of L&I 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.

The Licensing and Insurance (L&I) system was implemented under the authority of 49 U.S.C., Section 13902, titled "Registration of Motor Carriers," and 49 CFR 365, "Rules Governing Applications for Operating Authority." In addition, 49 U.S.C., Section 31138, titled "Minimum Financial Responsibility for Transporting Passengers," and Section 31139, titled "Minimum Financial Responsibility for Transporting Property" prescribes the minimum levels of financial responsibility required to be maintained by commercial motor carriers of property and passengers operating motor vehicles in interstate, foreign, or intrastate commerce.

L&I is the authoritative source for FMCSA licensing and insurance information and is a critical part of the registration process. L&I authorizes commercial motor carriers, freight forwarders, and property brokers from the United States, Canada, and Mexico for interstate commerce. L&I can also revoke this authority.

L&I only receives PII from owner-operators. The identifying information and credit card or bank check information provided by owner-operators is needed to process L&I application forms and to collect processing fees. Credit card/checking account numbers are required for payment of registration and administrative filing fees at the government electronic bill payment service (pay.gov). FMCSA does not collect, process, or store these financial transaction records, and records disposition is managed by the U.S. Department of Treasury.

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 collects, uses, and retains only that data that are relevant and necessary for the purpose of the L&I. The L&I system collects data from entities required to register with FMCSA as a sole proprietors, commercial motor carriers, freight forwarders, and property brokers.

Business information is collected from these entities when they register with FMCSA pursuant to Federal regulations. The business information allows FMCSA to positively identify those entities under its jurisdiction and manage FMCSA processes for which the information was collected. Owner-operator licensing and insurance records: Retention and

disposal of L&I records is managed in accordance with the NARA approved records disposition schedule for the L&I system (NI-557-01-1)[4].

Credit card/checking account numbers are required for payment of registration and administrative filing fees through the government electronic bill payment service (pay.gov), FMCSA does not collect, process, or store these financial transaction records, and records disposition is managed by the U.S. Department of Treasury.

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. The information collected in support of L&I allows FMCSA to positively identify entities under its authority and to process registration related fees. Additional administrative filings are required for certain motor carriers (for-hire) and brokers and freight forwarders, including evidence of financial responsibility (insurance) and a process agent designation. When filing the process agent designation, these entities must provide their business name, address, phone number and e-mail address. This information is available to members of the public for litigation purposes. Information collected for purposes of complying the URS final rule is not information protected under the Privacy Act; however, as discussed in the Overview section, because some business information may also be considered PII, the Department will implement policy to ensure that individuals are appropriately protected.

Authorized FMCSA personnel use L&I to enter licensing and insurance information. L&I also supports interactive entry of OP-1(MX) and OP-2 applications by border offices; entry of transferred data; selection of USDOT Numbers from the Motor Carrier Management Information System (MCMIS); retrieval of insurance and licensing letters; retrieval of name changes from the FMCSA registration system; and access to information concerning the status of commercial motor carriers, hazardous material (hazmat) shippers, and blanket companies.

Commercial motor carriers, freight forwarders, and property brokers use L&I to submit and track the status of applications for operating authority. Insurance companies, surety companies, and financial institutions use L&I to file certificates and cancellations; view their last transmissions; and print their confirmation, acceptance, and reject reports. L&I is also used to designate process agents (BOC-3) for commercial motor carriers, freight forwarders, and property brokers. In addition, anyone may query the L&I database to determine if a commercial motor carrier, freight forwarder, or property broker is active or inactive and if they have satisfied the requirements for registration. All information displayed in an L&I database query is public information that is available under FOIA and is provided free of charge.

Commercial motor carriers, freight forwarders, and property brokers may access their own licensing and insurance information in L&I with a valid USDOT Number or Docket Number, in addition to a Personal Identification Number (PIN).

Insurance companies, surety companies, financial institutions, and process agents may access L&I to file certificates and cancellations for their clients and to research potential clients.

[4] http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0557/n1-557-01-001_sf115.pdf

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 collection, use, and maintenance of information collected for operating the L&I system is relevant to the purposes for which it is to be used and, to the extent necessary for those purposes; it is accurate, complete, and up to date.

The L&I Customer Support Team reviews and approves all forms submitted by commercial motor carriers, freight forwarders, and property brokers. Forms are checked for completeness and verified for accuracy. Verification may include requesting legal documents directly from motor carriers, or from their agents or representatives.

Registered electronic filers may file certificates and cancellations; view their last transmissions; and print their confirmation, acceptance, and reject reports.

The redress process described in the Individual Participation and Redress section is a mechanism to maintain and improve accuracy of 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 L&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 L&I system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All records in the L&I system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the L&I system is logged and monitored.

Logical access controls restricts users of the L&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 L&I system. Any changes to user roles required 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 L&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/delete data commensurate with their requirements.

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

The L&I maintains 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 prevents unauthorized access to data stored in the L&I system. 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 to 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 L&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 L&I.

A security authorization is performed every year to ensure that L&I meets FMCSA and Federal security requirements. L&I also undergoes an additional security authorization whenever a major change occurs to the system. L&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. The L&I is approved through the Security Authorization Process under the National Institute of Standards and Technology. As of the date of publication of this PIA, the L&I was last authorized in July 31, 2015.

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 U.S. personnel and all AWS Cloud community customers are restricted to U.S. government entities from federal, state or local government organizations.

The AWS environment has 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 L&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 L&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 L&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 L&I.

Responsible Official

Betsy Benkowski
Office of Registration and Safety Information
Federal Motor Carrier Safety Administration
202-366-5387
Betsy.Benkowski@dot.gov

Approval

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