



U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

Unified Registration System (URS) Final Rule

Responsible Official

Steven Dillingham
Office of Registration and Safety Information
Federal Motor Carrier Safety Administration
202-366-3876
Steven.Dillingham@dot.gov

Reviewing Official

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

August 23, 2013



Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is developing and implementing the Unified Registration System (URS) Final Rule and associated system under the authority of section 103 of the ICC Termination Act of 1995 [Pub. L. 104-88, 109 Stat. 888, Dec. 29, 1995] and title IV of the Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU)[Pub. L. 109-59, 119 Stat. 1714, Aug. 10, 2005]. When deployed, the URS system will replace the Licensing and Insurance (L&I) System and the registration capability within the Motor Carrier Management Information System (MCMIS). The URS will serve as a clearinghouse and depository of information on, and identification of, all foreign and domestic motor carriers, motor private carriers, brokers, freight forwarders, and others required to register with the U.S. Department of Transportation, including information with respect to a carrier's safety rating, and compliance with required levels of financial responsibility. The FMCSA conducted this privacy impact assessment (PIA) because implementation of the URS Final Rule will result in the deployment of a system that will collect, store, and process business information that may also be considered personally identified information (PII).

Privacy Impact Assessment

The Privacy Act of 1974 articulates concepts for how the Federal Government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.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.

Unified Registration System (URS) Overview

The primary mission of the FMCSA is to reduce crashes, injuries, and fatalities involving large trucks and buses. This mission is accomplished by developing and enforcing data-driven regulations that balance motor carrier safety with industry efficiency; utilizing Federal and State safety information systems to focus on high-risk carriers and drivers to enforce safety regulations; targeting educational messages to carriers, commercial motor vehicle (CMV) drivers and the public; and partnering with stakeholders (e.g., Federal, State, and local enforcement agencies; the motor carrier industry; safety groups; and organized labor) to reduce bus- and truck-related crashes.

Current USDOT Registration Process

Under the current registration process for a new USDOT Number and Operating Authority, the Agency's responsibilities include monitoring and enforcing compliance with regulations governing both safety and commerce. Its focus on both concerns—safety and financial responsibility—is reflected in the dual path of its current registration process. Companies may find they are subject to both registration requirements—USDOT Number and Interstate Operating Authority—or either one separately. This dual path for registration process is achieved using two separate information systems:

Motor Carrier Management Information System (MCMIS)— All FMCSA regulated entities must self-identify by registering in MCMIS either through electronic or hard copy submission of the appropriate Motor Carrier Identification Report (Application for USDOT Number) MCS-150 series form to apply for a USDOT Number.² Obtaining a USDOT number is currently not required for freight forwarders or entities with existing operating authority, i.e., a docket number. There is no application fee when applying for a USDOT Number. FMCSA requires regulated entities submitting electronic applications to provide a valid credit card as part of FMCSA's fraud reduction strategy. Except for the last four digits of the card, the credit card information is not stored in any FMCSA system once the validation process has been completed. After completing the registration process in MCMIS, the entity receives a USDOT number and a personal identifier number (PIN) to allow online access to the system and updating of its registration information.

Licensing and Insurance (L&I) System— In addition to registering for a USDOT number in MCMIS, for-hire motor carriers, brokers, and freight forwarders must obtain operating authority from FMCSA by registering in the separate L&I System or hardcopy submittal using the appropriate Interstate Operating Authority (OP) series form.³ 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

² The MCS-150 forms may be found at <http://www.fmcsa.dot.gov/documents/forms/r-l/mcs-150-instructions-and-form.pdf> (Last accessed April 9, 2013)

³ OP series form may be found here - <http://www.fmcsa.dot.gov/documents/forms/r-l/op-1-instructions-and-form.pdf> (Last accessed, April 9, 2013.)

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. 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)⁴ 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 is 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, the BoA sends a copy of the canceled 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.

Motor carriers must update their MCMIS registration information every 2 years but a similar requirement to re-file or renew the commercial registration information for freight forwarders and brokers in L&I does not exist.

URS Final Rule

The URS Final Rule (Final Rule) requires all regulated entities (proprietor/driver⁵ or owner/operator of a motor carrier, intermodal equipment provider, freight forwarder, broker, hazardous materials safety permit holder or cargo tank facility) to register in the URS system using a new virtual Form MCSA-1 that combines data elements from the existing MCS-150 and OP series forms now used for registration in MCMIS and L&I. It will eliminate duplication and the guesswork involved in determining which form to complete. The user will complete only those portions of the Form MCSA-1 form that are applicable to its operations and bypass any irrelevant sections. When developed, URS will result in a more streamlined registration process.

With limited exceptions, the Final Rule requires all regulated entities to provide evidence of financial responsibility and to file a service of process agent designation, as a condition for registration. Formerly, only motor carriers, brokers and freight forwarders that were subject to its commercial oversight had to do so. The Final Rule explains who must register in URS, establishes a fee schedule for those entities who register, discloses all of the information the Agency will collect in URS and creates a list of cross-references to all other regulatory requirements for completing registration. Once the Final Rule is implemented all regulated entities must update their registration information every 2 years or be subject to new penalties.

⁴ 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 April 9, 2013)

⁵ A driver could be a sole proprietor or owner

Certain applicants⁶ must make two additional filings to complete registration: evidence of financial responsibility and process agent designation. The Final Rule requires all *for-hire* motor carriers (both exempt and non-exempt) under FMCSA safety jurisdiction, brokers and freight forwarders to file evidence of financial responsibility with FMCSA. Only private motor carriers who transport hazardous materials in interstate commerce are subject to this filing. Private non-HM carriers are not subject to this filing. Payment to register is completed before the insurance filing is made. All motor carriers (*private and for-hire*) under FMCSA safety jurisdiction, brokers and freight forwarders must file a process agent designation. Process agent designation filings are free of charge.

URS Registration Process

URS will consolidate the L&I System and the registration capabilities in MCMIS into a single, online registration system in which all FMCSA regulated entities must register; allowing FMCSA to discontinue the present paper-based registration process and transition to an exclusively electronic process. All regulated entities will be required to register for a new USDOT number and operating authority in the URS. The registration requirements for regulated entities will not change with the deployment of the URS only the system for completing them. The new Form MCSA-1 will eliminate collection of duplicate information and decrease the burden on applicants by eliminating the need for each applicant to determine which forms they must complete. When developed, the URS will introduce efficiencies into the registration process applying business logic so only those questions pertinent to the applicant will be presented for completion and automatically bypass all non-relevant Form MCSA-1 questions and certifications. The result is a streamlined registration process, enabling the Agency to more efficiently monitor the safety performance of its regulated population and increase public accessibility to data maintained by FMCSA on regulated entities.

Under the URS application process, a new applicant will be issued an inactive USDOT Number. The inactive USDOT Number will be activated by FMCSA only after it has determined that the applicant is willing and able to comply with applicable regulatory requirements and the applicant has satisfied applicable administrative filing requirements, such as evidence of financial responsibility, if applicable, and a process agent designation. All regulated entities will be required to complete administrative filing requirements in the URS.

Information Collected in URS

The URS system collects business information from regulated entities identified in the URS Final Rule required to register with FMCSA as a sole proprietor. The URS system collects the following information from covered entities registering in the system:

- Business name,
- Address,
- Email address,
- Employer Identification Number (EIN)⁷,

⁶ Intermodal equipment providers, hazardous materials safety permit holders, and cargo tank facilities are required to maintain financial responsibility and maintain evidence of insurance at their place of business. They do not have to file evidence of financial responsibility or complete a process agent designation filing unless they are also a motor carrier.

⁷ Additional information about applying for an Employer Identification Number (EIN) on the Internal Revenue Service website - [http://www.irs.gov/Businesses/Small-Businesses-&Self-Employed/Apply-for-an-Employer-Identification-Number-\(EIN\)-Online](http://www.irs.gov/Businesses/Small-Businesses-&Self-Employed/Apply-for-an-Employer-Identification-Number-(EIN)-Online). (Last accessed April 9, 2013)

- Credit card number, and
- Checking account number.

FMCSA requires regulated entities to disclose their EIN for the purposes of uniquely identifying each regulated entity in the system and uses the registration information to validate other business information provided on the URS application form (Form MCSA-1). A large portion of FMCSA regulated entities are sole proprietors who may use their personal information as business information. Sole proprietors who do not obtain an EIN may instead provide their social security numbers (SSN) instead of the EIN. However, the Agency strongly encourages sole proprietors to obtain an EIN. The Agency will continue to permit a sole proprietor to provide its social security number (SSN) in lieu of the EIN.

While information submitted by some regulated entities may also constitute personal information, this information is submitted as business information and is not statutorily protected by the Privacy Act of 1974. However the Department of Transportation recognizes that the unauthorized access and/or use of this information could have serious repercussions for individuals and therefore has implemented a privacy protection program for the URS system and associated activities.

In addition to the information collected in support of registration applications, the URS requires regulated entities to establish user accounts to update their registration information through the FMCSA Portal (www.fmcsa.dot.gov). The FMCSA Portal is a web-enabled system designed to authenticate users to various FMCSA IT Systems. Users will log into the FMCSA Portal to access the URS. The PIA for the FMCSA Portal is currently under development. When the PIA is developed, it will be published on the DOT website at <http://www.dot.gov/privacy>.

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.

FMCSA does not secretly collect or store PII and will clearly disclose its policies and practices concerning the PII collected and held associated with the implementation of this Final Rule. FMCSA has provided generalized notice to the public through the information practices associated with the implementation of the URS Final Rule. The FMCSA published the Form MCSA-1 and instructions in the October 26, 2011, Supplemental Notice of Proposed Rule Making (SNPRM) (FR Volume 76, 207, October 26, 2011) for the

URS and fully disclosed the information that will be collected and stored in the URS. Nine entities responded to the SNPRM, some of which included comments about the Form and instructions, but none were received concerning privacy. The FMCSA response to these comments and any changes to Form MCSA-1 and instructions will be published in the URS Final Rule.

Specific notice will be given to regulated entities prior to their provision of information to the URS system. Registrants must provide explicit consent including that they are willing and able to comply with FMCSA requirements, and that they agree abide by the URS/FMCSA Terms of Use and Privacy Policy.

Publication of this PIA further demonstrates DOT/FMCSA's commitment to provide appropriate transparency and may be found on the DOT Privacy Office website (www.dot.gov/privacy) as well as part of the URS rulemaking docket (Docket FMCSA-1997-2349).

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.

The URS Final Rule requires registered entities to update registration information not less than every 2 years. The URS system will include capabilities to allow regulated entities to modify, correct, and update registration information maintained in the *whenever necessary*, free of charge. Also, pursuant to 49 U.S.C. 13908(c), as amended by section 4304 of the Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU), the FMCSA redress management systems (DataQs)⁸ provides an electronic means to file concerns about Federal and State data that FMCSA makes publicly available. 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. The DataQs process also allows filers to monitor the status of each filing.

Statutory Authority and Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

The Unified Registration System (URS) is being developed and implemented under the authority of section 103 of the ICC Termination Act of 1995 [Pub. L. 104-88, 109 Stat. 888, Dec. 29, 1995] and title IV of the Safe, Accountable, Flexible, and Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU)[Pub. L. 109-59, 119 Stat. 1714, Aug. 10, 2005]. Congress intended for URS to serve as a

⁸ A discussion of the DataQs privacy program may be found on the DOT Privacy website (www.dot.gov/privacy).

clearinghouse and depository of information on, and identification of, all foreign and domestic motor carriers, brokers, and freight forwarders, and other entities required to register with the Department as well as information on safety fitness and compliance with minimum levels of financial responsibility. (U.S.C. 13908(b)).

Motor carriers (private and for-hire), brokers, freight forwarders, intermodal equipment providers, and cargo tank facilities register with the Agency to obtain a USDOT identification number. Certain motor carriers, brokers and freight forwarders additionally fall under FMCSA commercial oversight and register with the Agency to obtain authority to operate in interstate commerce (operating authority). Entities that transport certain high hazardous materials identified in 49 CFR § 385.405 of the FMCSRs register to obtain a hazardous materials safety permit and USDOT Number.

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 URS. The URS collects data from entities required to register with FMCSA as a sole proprietor/driver or owner/operator of a motor carrier, intermodal equipment provider, freight forwarder, broker, or cargo tank facility.

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. Credit card/checking account numbers are required for payment of registration and administrative filing fees through the government electronic bill payment service (pay.gov), but this information is not retained in the URS.

The DOT/FMCSA records schedule for the URS records was submitted to the National Archives and Records Administration (NARA) for approval in February 2012 under Job Number DAA-0577-2013-0003. All records maintained in the URS will be treated as permanent records until the schedule is approved by NARA. The proposed schedule includes the following retention periods for records containing PII: (1) inputs, such as, motor carrier registration, compliance review ratings, and other related motor carrier safety performance and compliance information will be destroyed or deleted, regardless of media, after information is converted or copied to the URS master data files, backed up, and verified; (2) master data files – historical copy will be cut off at end of fiscal year, and transferred to the National Archives 3 years after cut off; (3) master data files – record copy will be deleted or updated when data is superseded or obsolete; and (4) outputs, such as, regular safety, statistical, or management reports and ad hoc reports will be cut off when report is run and filed to a separate recordkeeping system and use that recordkeeping system's disposal authority. Record output issuances that are not filed to a separate recordkeeping system will be destroyed or deleted 36 months after issue run or when no longer needed for reference, 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. The information collected in support of implementation of the URS Final Rules 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: 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 because some business information may also be considered PII the Department will implement appropriate policy to ensure that individuals are appropriately protected.

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 implementing the URS Final Rule 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. Regulated Entities were provided an opportunity to recommend changes and updates to Form MCSA-1 and instructions during the 60-day comment period for the SNPRM. URS will comply with applicable FMCSA security standards, include data checks to ensure that information collected conforms to formatting requirements (i.e., nnn-nn-nnnn for EIN), and require completion of certain fields as a condition of proceeding to the next section of the application where appropriate. Entities sometimes use agents to register with FMCSA. Entities registering with FMCSA who provide business information electronically, or their agents, will be responsible for its accuracy.

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.

Logical access controls will restrict users of the URS. These controls will be guided by the principles of least privilege and need to know. Users accounts will be created with specific job functions and

accounts will be granted the necessary access to perform their role as approved by the System Manager. Any changes to user roles will require approval of the System Manager.

The URS will maintain an auditing function that tracks all user activities in relation to data including access and modification. Through technical controls including firewalls, intrusion detection, encryption, access control list, and other security methods. FMCSA will prevent unauthorized access to data stored in its URS. These controls will meet Federally mandated information assurance and privacy requirements.

Authorized DOT employees and contractors will have password-protected access to the system to perform their official duties including system administration, monitoring, security functions as well as viewing and verifying the registration information. Access to the registration information will be limited to authorized representatives of FMCSA or authorized Federal, State, or local enforcement agency representatives. The secure system will encrypt all documents.

Government Personnel and contractors are required to attend security awareness and privacy training offered by DOT/FMCSA and role-based training. This will allow individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use business information in the course of performing their duties. Access will be automatically restricted by systems and policies with oversight conducted by the IT Security Officer and management level government personnel. No access will be allowed prior to receiving the necessary clearances and training as required by DOT/FMCSA.

The URS will undergo the security authorization process under the National Institute of Standards and Technology no later than 60 days prior to the system becoming fully operational.

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 implementation of the URS rule. 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 and Privacy Officers will conduct regular periodic security and privacy compliance reviews of the URS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Responsible Official

Steven Dillingham
Office of Registration and Safety Information
Federal Motor Carrier Safety Administration

Approval and Signature

8/23/2013

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

X Claire W. Barrett

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

DOT Privacy Office - Approved -