U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

Unified Registration System (URS)

Responsible Official

Jeff Secrist
Jeff.Secrist@dot.gov
202-385-2367

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an Operating Administration (OA) 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 Unified Registration System (URS), an electronic on-line registration system that streamlines and simplifies the FMCSA's registration process for first time applicants, including motor carriers, brokers, freight forwarders, intermodal equipment providers (IEPs), hazardous materials safety permit (HMSP) applicants/holders, and cargo tank manufacturing and repair facilities.

This Privacy Impact Assessment (PIA) is published in accordance with the E-Government Act of 2002 and addresses the risks associated with maintaining and facilitating access to data in the URS. The URS collects personal and business information that may also be considered Personally Identifiable Information (PII).

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

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

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*

DOT Privacy Office Approved - 02/05/2025

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

- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

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

Introduction & System Overview

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 enforcements agencies; the motor carrier industry; safety groups; and organized labor) to reduce bus- and truck-related crashes.

Former USDOT Registration Process

Under the 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. The last four digits of the applicant's credit card numbers are stored encrypted in FMCSA's system after the validation process is completed. Broader credit card information is stored encrypted after validation.

[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).

DOT Privacy Office - Approved - 02/06/2025

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 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 processes 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 and security information[5] 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 and security information are deleted after the operating authority transaction payment process has been completed. Checking account information and the last four digits of the credit card number is stored to provide FMCSA a means to trace unauthorized 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 U.S. Bank for processing. Once the payment is processed, U.S. Bank 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 two 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.

DOT Privacy Office - Approved - 02/06/2015

[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.)

[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] Security information includes: the URS Application Password, The Company Official Portal Password, and answers to security questions for both the URS Applicant and the Company Official.

Current URS Registration Process

The URS integrates the online registration application process from L&I System and the MCMIS into a single, online platform. The URS only allows first-time applicants to register for a USDOT number and, if applicable, Operating Authority. Existing regulated entities (e.g., those already possessing a USDOT number) must use the L&I system to add or update their Operating Authority and MCMIS to update their USDOT registration information.

When first-time applicants submit their initial registration application in the URS, the system synchronizes the provided information with MCMIS to create a new USDOT record and with L&I to establish a new docket number record (e.g., MC/FF/MX docket numbers) if Operating Authority is required. The deployment of URS has not changed the registration requirements for regulated entities; it has simply modernized the system for completing these requirements by transitioning to an exclusively electronic process.

The URS utilizes Form MCSA-1, which consolidates the MCS-150 and OP-1 series forms, eliminating duplicate data collection and reducing the burden on applicants. By applying business logic, the system presents only questions relevant to the applicant's registration, bypassing non-relevant questions and certifications, effectively streamlining the registration process.

Under the URS application process the URS issues an active USDOT number and, if required, places the docket number in a pending status for Operating Authority applications. Operating Authority is activated by FMCSA only after confirming that the applicant meets all regulatory and administrative requirements, including providing evidence of financial responsibility and process agent designation.

Existing regulated entities are required to maintain and update their company information in MCMIS for their USDOT registration and in L&I for Operating Authority to ensure compliance with FMCSA regulations and facilitate the monitoring of safety performance and public data accessibility.

Identity Verification Service

FMCSA developed a process by which individuals can begin their registration through URS after verifying their identity through an Identity Verification Service (IVS) provided by a third-party vendor, IDEMIA Identity & Security USA LLC (IDEMIA). Individuals wishing to register will be redirected to an identity verification application maintained by the vendor The vendor’s IVS provides enhanced identity verification for URS users, which must be completed before FMCSA issues a new registration through URS. This verification process is an important fraud prevention tool which helps ensure that only authenticated individuals or entities register through URS. The vendor manages the PII provided in accordance with

DOT Privacy Office - Approved 07/06/2025

its privacy policy[6], which includes the collection, processing, and storage of personal and biometric information and identifiers (e.g., facial imaging) necessary to perform liveness verification and credential match. This means that all personal information collected during the identity verification process is handled by the vendor and not stored or managed by FMCSA.

The vendor's IVS supports omni-channel onboarding. This means customers may use different channels such as remotely using a smartphone, tablet, or personal computer, or alternatively, in-person assistance via agents, to verify their identity. To complete the verification process, a customer must 1) transmit a photo of a valid state-issued Driver's License or other acceptable forms of identification and 2) use their personal mobile device for facial recognition verification. IVS then validates the customer's form of identification, confirms the identity of the individual, and compares the results with data in their existing databases. Customers who are unable or unwilling to verify their identity using digital means (e.g., mobile phone or computer), may go in-person to one of the sanctioned enrollment centers and undergo the process of identity verification with the assistance of an agent. The vendor sends the results of the verification (verified or not verified) to FMCSA allowing the customer to move forward with the registration process. Once the verification process is complete, the vendor deletes any collected PII and shares the transaction result with FMCSA. The result does not include any PII. Once the IVS is implemented with URS, FMCSA will extend the service to include all existing registrants wishing to make changes to their registration record via L&I, and registrants who submit paper applications to the FMCSA Contact Center.

DOT Privacy Office - Approved 02/06/2025

Personally Identifiable Information (PII)

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:

- Sole Proprietor's Name,
- Business name,
- Sole Proprietor's Address,
- Business Address,
- Telephone number,
- Email address,
- Employer Identification Number (EIN)[7],

[6] https://www.idemia.com/privacy-policy

[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).

- Credit card number,
- Checking account number
- Login credentials (i.e., username and password), and
- DUNS number.

The Identity Verification Service (IVS) collects PII from individuals who are required to register with FMCSA. The IVS collects the following information as part of the identify verification process:

- Name
- Date of Birth
- Address
- Passport
- Driver's License

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 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 log into the FMCSA Portal to access the URS.

DOT Privacy Office - Approved - 02/06/2025

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states,

as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[8], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[9].

Transparency

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

FMCSA does not secretly collect or store PII and will clearly disclose its policies and practices concerning the PII collected and held associated with the URS. FMCSA provided generalized notice to the public through the information practices associated with the implementation of the URS Final Rule (https://cms.fmcsa.dot.gov/regulations/final-rule-unified-registration-system). 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 was published in the URS Final Rule.

Specific notice was 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.

FMCSA's use of information stored in URS is addressed 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

DOT Privacy Office Approved: 02/06/2025

[8] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[9] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

(http://www.gpo.gov/fdsys/pkg/FR2013-09-25/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.

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 provides 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 they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

FMCSA provides a process for individuals to seek redress regarding inaccuracies in their registration application census information, such as legal and/or doing business as (DBA) names, physical (principal place of business or PPOB) and/or mailing addresses, and telephone numbers. During the application process, any necessary modifications to an individual's information must be addressed by contacting FMCSA for manual intervention. Individuals may be required to update the relevant forms (e.g., MCS-150 and/or OP-1 series forms) and submit supporting documentation for FMCSA validation to process their request.

Once a USDOT number or Operating Authority registration has been granted, individuals must submit the appropriate forms (e.g., MCS-150 series or Form MCSA-5889) to correct their census or company information in MCMIS or L&I. Alternatively, they may access their FMCSA Portal (https://portal.fmcsa.dot.gov/login) account using their Login.gov credentials to make updates online.

Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), individuals may request searches of the authoritative sources 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

DOT Privacy Office - Approved - 02/06/2025

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 it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

The URS was 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 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)).

Regarding registration in URS, 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.

FMCSA collects, uses, and retains only that data that is 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. The proposed schedule includes the following retention

DOT Privacy Office - Approved - 03/06/2025

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 the URS system 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 in URS 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 implements 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 in the URS 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. URS complies with applicable FMCSA security standards, include data checks to ensure that information collected conforms to formatting requirements (i.e., nnn-nn-nnnn for EIN). In addition, URS requires completion of certain fields as a condition of proceeding to the next section of the

DOT Privacy Office - Approved - 02/06/2025

application where appropriate. Entities sometimes use agents to register with FMCSA. Entities registering with FMCSA who provide business information electronically, or their agents, are 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 to 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 restrict users of the URS. These controls are guided by the principles of least privilege and need to know. Users accounts are created with specific job functions and accounts are granted the necessary access to perform their role as approved by the System Manager. Any changes to user roles require approval of the System Manager.

The URS 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 its URS 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.

Authorized DOT employees and contractors 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 is limited to authorized representatives of FMCSA or authorized Federal, State, or local enforcement agency representatives. The secure system encrypts all documents.

Government Personnel and contractors are required to attend security awareness and privacy training offered by DOT/FMCSA as well as role-based training. This 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 business information while performing their duties. Access is automatically restricted by systems and policies with oversight conducted by the IT Security Officer and management level government personnel. No access is allowed prior to receiving the necessary clearances and training as required by DOT/FMCSA.

DOT Privacy Office - Approved - 12/06/2025

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 follows the Fair Information Principles as best practices for the protection of information associated with URS. In addition to these practices, policies and procedures are consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance is 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 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

Jeff Secrist
URS System Owner
Federal Motor Carrier Safety Administration

Prepared by: Pam Gosier-Abner

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.02.06 14:05:01 -05'00'

DOT Privacy Office - Approved 02/06/2025