U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)
Customer Insurance and Registration Information Support (CIRIS)

Responsible Official

Vivian Oliver
Transportation Specialist
202-366-2974
Vivian.Oliver@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: 2018.09.13 15:16:13 -04'00'

Executive Summary

The Department of Transportation's (DOT) Federal Motor Carrier Safety Administration's (FMCSA) is a core mission is to reduce commercial motor vehicle-related crashes and fatalities. FMCSA's Office of Registration and Safety Information (MC-RS) houses the Agency's motor carrier and related entity registration, licensing, insurance, vetting functions, along with various customer service/contact center efforts. FMCSA receives, processes, stores, analyzes, researches, and disseminates safety, licensing and registration data for interstate and intrastate motor carriers, shippers of hazardous materials, and other motor carrier-related entities in the U.S, Canada, Mexico, and other non-U.S based carriers. To do this, FMCSA has acquired RightNow, a ommercial off-the-shelf, cloud based systemCustomer Relationship Management (CRM) tool to support the activities of its Customer Insurance and Registration Information Support (CIRIS) program. This Privacy Impact Assessment (PIA) is necessary to provide information regarding the use of the CRM within the MC-RS customer service program, and evaluates the privacy risks and mitigations associated with the collection, use, and maintenance of Personally Identifiable Information (PII) collected from memebrs of the public.

What is a Privacy Impact Assessment?

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

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

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

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

[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).

Introduction & System Overview

FMCSA receives, processes, stores, analyzes, researches, and disseminates safety, licensing, and registration data for interstate and intrastate motor carriers, shippers of hazardous materials, and other motor carrier-related entities in the United States (U.S.), Canada, Mexico, and other non-U.S. based carriers. In December of 2014, FMCSA established a new customer service contract replacing its telephone call center with a new multi-channel contact center solution that utilizes the cloud-based, RightNow, customer relationship management (CRM) tool. The major CIRIS functions supported by the CRM include registration, licensing and insurance customer service, data entry and dissemination, and report building.

The primary purposes of this solution were to address the following agency needs:

- Tracking of data dissemination requests by customer service agents (CSA) on behalf of the agency
- Creation of a central repository for customer interations to better facilitate registration, licensing, vetting and enforcement efforts
- Creation of a unique Customer Contact Record for each customer. The Record is available to all CSAs. The record includes all inquiry responses facilitating consistency across engagements and limiting opportunities for “answer shopping”.
- Improvement of records management as customer submissions are now a part of a record that links inquiries with agency actions and correspondence
- Expansion of customer egnagement platforms to to include email, web form submissions, chat, and co-browsing[2], in addition to phone, fax and mail.

CRM Workflow

The CRM is used to capture all interactions with CIRIS and CSAs regardless of the platform used by the customer to initiate their inquiry. All customer service engagements result in the creation of or an update to a Customer Contact Record. All inquires are assigned a unique ticket number which are then assigned to CSAs to research resolve and provide responses. The tickets are assigned in the order in which they are received. The system captures the time and date of the ticket, along with the caller’s contact information (name, company, phone, email, address, DOT#). The name of the assigned CSA and any information they include regarding the inquiry, its resolution, and the engagement is also added to the ticket as the CSA works to resolve the customer’s issue.

The CRM has been integrated with the CIRIS fax and phone system. When a customer calls or faxes the CRM automatically checks the customer database to determine if the phone or fax number is already known to CIRIS and associated with a customer file. If the customer already has a CIRIS engagement on file a new ticket is created and populated with the customer profile. If the customer is not previously known to CIRIS, the CRM will create a new master customer service record and generate a new ticket populated with the phone/fax number. A similar process is initiated when a customer emails or intiates an inquiry using one one of the webforms hosted on the FMCSA web site (www.dot.gov/fmcsa) except the CRM uses the customer email address to search the customer database.

CIRIS Quality Assurance

The FMCSA quality assurance program allows FMCSA to provide oversight of the CIRIS program, ensure the consistency and conformity with FMCSA regulations of responses, and continuously improve its customer service. At the conclusion of each engagement the FMCSA provides the customer an opportunity to provide feedback on the process

[2] Co-browsing technologies allows customers to permit FMCSA customer service agents temporary remote access the customer web-brower. Once access is established the FMCSA

and the information provided. Customer satisfaction surveys are sent via email to all customers who provide their email address.

CIRIS also uses a call-center management tool, ASTERNIC, which captures call-center performance metrics (calls were abandoned, how many answered, by whom, call duration, etc., for FMCSA analysis. The contractor also uses ATERNIC to record and store customer calls. Stored calls are reviewed on an ad-hoc basis by FMCSA management and contractor supervisors for quality assurance. Additionally as part of the quality assurance program, FMCSA staff and contractor supervisors may listen to "live" calls to provide more immediate support or feedback to CSA agents.

The CRM software solution provided by FMCSA contractor also allows customers access to online self-service options where they have access to a FAQ knowledge base that provides the top five answers by topic and allows the user to rate the effectiveness of the resolution (so the feature can be continuously improved). The CRM also includes a web form configured to suggest FAQs before allowing the end-user to initiate a web chat or email, further reducing the need to directly engage with CSAs.

Personally Identifiable Information and CIRIS

The During the customer service contact, CIRIS staff may request information from the indivdual to assist with registration related questions and issues. The specific data elements collected are dependent on the nature of the interaction but reflect the information typically found in standard FMCSA Forms. Information collected may include:

- Contact Information
  - Name,
  - Address,
  - Phone number(s),
  - Email address(es),
  - Fax Number
- Social security number
- Commerical Drivers License (CDL) Number
- Carrier/Employer
  - Employer identification number
  - Commercial Motor Vehicle (CMV) Number
- Credit Card
  - Credit card number and expiration date
  - Credit card account holder name

Calls recorded and maintained in ASTERNIC are indexed by call date and the integrated review tools allows users to sort records by only displays the incoming call number, the CSA name and call queue. PII made available during the call is caputred in the call recording and as appropriate transcribed into the customer record maintained in the CRM but is not captured as discrete data fields in the ASTERNIC system.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template based on the fair information pratice 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[3], 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[4].

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.

CSAs notify all callers that phone calls may be recorded for quality assurance and that telephone numbers may be used to contact the customer about their customer service experience.

Records in the system will be protected in accordance with DOT/FMCSA 010 – Customer Insurance Registration Information Support (CIRIS) system of records notice (SORN). The SORN will be available to the public on the DOT Privacy Office website www.transporation.gov/privacy. and from the Federal Register (www.federalregister.gov).

FMCSA informs the public that their PII is stored and managed in the CRM through this PIA, published on the DOT website, www.transporation.gov/privacy. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, along with all uses of the PII stored and transmitted through the CIRIS system.

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 CIRIS support allows individuals to directly engage with the customer service agents to amend an their file.

Individuals seeking access or amend their CRM records may file a Freedom of Information Act (FOIA) request by sending a written request directly to:

Federal Motor Carrier Safety Administration
Attn: FOIA Team MC-MMI

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

1200 New Jersey Avenue SE
Washington, DC 20590

If an individual wishes to access or amend records that the FMCSA maintains that are protected under the Privacy Act concerning him or her, the individual may submit the request to:

Departmental Freedom of Information Act Office
ATTN: FOIA request
U.S. Department of Transportation, Room W94–122
1200 New Jersey Ave. SE.
Washington, DC 20590

When seeking records about yourself from the CRM or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 49 CFR Part 10. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Freedom of Information Act Officer, *http:// www.dot.gov/foia* or 202.366.4542. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DOT component agency may have responsive records; and If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records. Without this bulleted information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

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.

FMCSA receives, processes, stores, analyzes, researches, and disseminates safety, licensing and registration data for interstate and intrastate motor carriers, shippers of hazardous materials, and other motor carrier-related entities. Information is collected directly via phone call, fax, web form and mail.

This information is collected and stored to create a centralized repository of carrier records and communications to better serve carriers seeking status updates on various registration related transactions, ensure the agency provides consistent guidance as agents and FMCSA personnel can now easily see the notes and transaction details for each caller, and provide detailed, up-to-date records for FMCSA's vetting and enforcement users. Additionally, the data is made available to CMV companies that use the information for educational, legal, or safety analysis purposes.

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.

The FMCSA has prepared a records dispostion schedule for the CIRIS system that will be submitted to NARA for approval. All records maintained in this system of records are treated as permanent records until the schedule is approval by NARA.

FMCSA collects, uses and retains only that data that are relevant and necessary for the purpose of the CRM. Records in the CRM may be retrieved by; individuals' name, address, email address, and telephone number.

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.

CIRIS support may request information from the individual to further assist with questions and issues, including authentication. Used to confirm information that is already in our system. authrenticate in writing or online for request for data changes The specific data elements collected are dependent on the nature of call. Information collected may include: driver name, email address, and telephone number. In addition all inbound calls to the CIRIS support are recorded for quality monitoring and customer satisfaction assurance purposes. The recorded content may contain PII (based upon the nature of the conversation).

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 CIRIS support ensures accuracy by collecting information directly from the individual. Callers are required to authenicate themselves before service can be granted. To complete authentication, customer service agents may either use the reference number provided from FMCSA correspondence, the confirmation number provided when the individual submitted a web form, or if neither apply, the agent can create a new incident record.

If the correspondence number, confirmation number or basic demographic data (such as company name, address, or phone number) is provided and the system finds a match, the CSA asks questions to validate the caller's identity and assist with the inquiry, preventing unauthorized disclosure of information. These questions include asking additional questions that are likely only known to the individual, such as name, DOT or MC number, email address, or the principal address for the businss. Each inquiry creates a record which also allows the agency to relate incidents and merge records to maintain a more up-to-date and accurate archive by reducing duplicate records and linking multiple inquiries.

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. 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009. 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 CRM 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 records 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 or permissions. The CRM employs role-based access controls and privileges based on whether the user is an FMCSA employee or CIRIS support contract. Such authorized users may read, add, and modify a commensurate with their role.

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

The CRM is approved through the Security Authorization Process under the National Institute of Standards and Technology. After a review of the security and privacy controls, the CRM was issued an Authority to Operate on June 30, 2015.

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 Practice Principles as best practices for the protection of information associated with the CIRIS 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 CRM consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Audit provisions are also included to ensure that the CIRIS system and the CRM solution are 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 the CRM. FMCSA

contractors involved in data analysis and research are also required to sign the FMCSA Non-Disclosure Agreement prior to being authorized to support the CIRIS System.

Responsible Official

Vivian Oliver
Transportation Specialist
202-366-2974
Vivian.Oliver@dot.gov

Approval and Signature

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