



U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration (NHTSA)

Child Restraint System (CRS) Registration Collection

Responsible Official

Cristina Echemendia
General Engineer
Special Vehicle and Systems Division
Office of Rulemaking
1-888-327-4236
www.nhtsa.dot.gov

Reviewing Official

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



Executive Summary

The Federal Motor Vehicle Safety Standard No. 213, “Child Restraint Systems (CRS),” requires CRS manufacturers to provide different registration methods to the owners of child restraint systems so that they may be directly contacted in a recall campaign. The methods include providing a two-part perforated registration card and a permanently attached label on the CRS. NHTSA provides a substitute registration form (OMB No. 2127-0576) on its website, which consumers can send their CRS registration to NHTSA for forwarding to the manufacturer. The substitute form is provided with the goal of increasing the number of CRSs that are remedied in a recall, in line with NHTSA’s mission to save lives, prevent injuries, and reduce vehicle-related crashes. NHTSA forwards the form that are submitted to the appropriate manufacturer.

A Privacy Impact Assessment (PIA) is required because the form contains personally identifiable information (PII) on members of the public. As this system meets the requirements of the Paperwork Reduction Act (PRA), NHTSA ensures that the requirements of the PRA are met and follows the appropriate channels for Office of Management and Budget (OMB) approval.

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.

Introduction & System Overview

The Federal Motor Vehicle Safety Standard No. 213, “Child Restraint Systems (CRS),” requires CRS manufacturers to provide different registration methods to the owners of CRSs so that they may be directly contacted in a recall campaign. Specifically, the standard requires:

- (a) A two-part perforated registration card. The first part contains a message and instructions to be retained by the purchaser. The second part is to be returned to the manufacturer by the purchaser. The second part includes prepaid return postage, the pre-printed name/address of the manufacturer, the pre-printed model and date of manufacture, and spaces for the purchaser to fill in his/her name and address and optionally email-address;
- (b) A permanently attached label on the CRS, which includes a statement providing mailing and telephone instructions (or, at the option of the manufacturer, a toll-free hotline telephone number) for non-original owner registration and for re-registration, and the U.S. Department of Transportation’s Auto Safety toll-free hotline number for reporting and receiving safety-related information about the CRS; and
- (c) A filing system containing CRS owners’ names and addresses is maintained by the CRS manufacturer. This system must be suitable for easy access in the event of a recall campaign. The registration records are to be maintained by the manufacturer for 6 years.¹ Manufacturers are required to maintain a file system of this information of their choice, but the standard does not require the use of electronic records.² If a defect or compliance problem exists with a CRS, the manufacturer is able to search its records to locate and contact consumers owning the same model of the defective CRS.

FMVSS No. 213 permits information regarding online product registration to be included on the owner registration form required under the standard. As NHTSA seeks to increase the number of CRSs that are remedied and strives for better recall compliance, the CRS registration information enables manufacturers to directly contact CRS owners to notify them of safety recalls. This better ensures that owners will hear about a recall and remedy the safety problem with their CRSs. Manufacturers are also permitted to supplement (but not replace) recall notification via first-class mail with e-mail notification, which increases the likelihood that owners learn of a recall.

In order to ensure that CRS owners are provided with the greatest number of opportunities to be notified of recalls, NHTSA provides a substitute registration [form on its website](#).³ This printable form includes registration information, CRS make, model and manufacturing date to NHTSA. The form has a statement authorizing the agency to provide the CRS registration information to the manufacturer. Since child restraint registration is left up to the individual, NHTSA is involved in the process to help facilitate registration. The option to fill out the form via the website is helpful for families that have second hand CRSs. They are able to ensure that the CRS is properly registered to them. Additionally, child passenger safety technicians are able to provide the form found on the website at car seat inspection stations. The Office of Research and Program Development received input from partners and child

¹ 49 CFR 588.6 states: “Each manufacturer, or manufacturer's designee, shall maintain the information specified in § 588.5 of this part for a registered restraint system for a period of not less than six years from the date of manufacture of that restraint system.”

² 49 CFR 588.5 states: “Each manufacturer, or manufacturer's designee, shall record and maintain records of the owners of child restraint systems who have submitted a registration form. The record shall be in a form suitable for inspection such as computer information storage devices or card files, and shall include the names, mailing addresses, and if collected, se-mail addresses of the owners, and the model name or number and date of manufacture (month, year) of the owner's child restraint systems.”

³ <https://www-odi.nhtsa.dot.gov/recalls/register/childseat/csregfrm.pdf>

passenger safety technicians across the country that this option allowed them to do registrations for families that do not have access to the internet. Additionally, having the option to register seats with families at the actual inspection station may increase the likelihood that some of the higher risk families served by the inspection stations register their seats. This has the potential to increase recall compliance

NHTSA receives approximately 1,200 substitute registration forms per year. Forms are received by mail, fax, and email. When a form is received, an on-site contractor converts the paper registration card to an electronic form and saves all documents to a NHTSA server. The form is emailed to the manufacturer as they are received. The scanned copies are stored for 30 days and then deleted. While stored, these copies can only be retrieved by manufacturer name. The physical copies received by mail or fax are placed in locked disposal bins until destroyed.

Personally Identifiable Information (PII)

The substitute form asks for the following information:

- Email
- Name
- Address
- City, State, and Zip
- Child Seat Manufacturer
- Model Number
- Manufacturer Date

NHTSA realizes there is privacy risk in collecting the information on members and the public and that ideally, the form should be sent directly to the manufacturer to minimize risk. NHTSA will examine other methods whereby the form will be sent directly to the manufacturer.

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 personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

NHTSA has received authority for this collection under OMB 2127-0576 and it was last approved on April 2nd, 2015.⁴ The forms are not maintained in a system of records, as they are not retrieved by a unique identifier associated with an individual. After a form is emailed to the manufacturer, a copy is saved. This copy is indexed by manufacturer name and may only be retrieved by manufacturer name. While the records do not fall under the Privacy Act, they are maintained in accordance with DOT Privacy Policy and the FIPPs to minimize the risk associated with the collection of the forms and to protect the privacy of members of the public.

NHTSA also informs the public that their PII is collected and stored through this Privacy Impact Assessment, and published on the DOT website. This document identifies the information collection's purpose, storage, and use of the PII. The 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.

The form states the purpose of the collection and includes the OMB approval number (OMB No. 2127-0576). NHTSA does not verify the information provided by the consumer. All information provided on the form is securely emailed to the manufacturer, and destroyed after 30 days.

Should an individual have any questions about the process or the form, the form provides contact information for a Hotline (1-888-327-4236) and a website (www.nhtsa.dot.gov). If an individual needs to make changes or updates to the form, they will need to submit a new form, or contact the manufacturer directly. Additionally, an individual can contact a responsible NHTSA staff member to address privacy concerns by writing to NHTSA.Privacy@dot.gov.

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 it collects, uses, maintains, or disseminates PII.

While the form is not required by statute, it provides consumers with an alternative method of registering their child restraint system with the aim of increasing the number of CRSs that are remedied in the event of a recall. Child passenger safety technicians can provide the printed form to those who may not have access to the internet. The consumers are expected to complete the form themselves. The option to download and print the form from the website is also helpful for families that have second-hand CRSs. It ensures that their CRSs are properly registered to them.

The PII collected on the form is for the sole purpose of registration of the CRS with the manufacturer. It is not used by NHTSA for any other purpose.

⁴ RegInfo.gov: https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201408-2127-004

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.

NHTSA aims to increase the number of CRS that are remedied in the event of a recall. Whereas vehicles are registered at the state level, and easier to track, CRSs are not. As such, NHTSA is involved in the process of registering CRSs by providing the form and an alternative means of registration. All information is passed directly to the manufacturer of the CRS. The substitute registration form contains only the information as described above and it does not request or require any additional information. NHTSA in no way uses the information for its own purposes. To reduce the risk associated with the collection of PII, NHTSA is in the process of developing a records retention schedule that will specify that the records will only maintained for 30 days .

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.

When NHTSA receives a form, it forwards it to the manufacturer. NHTSA sends all information that it receives forward to the manufacturer so that the manufacturer may contact a consumer in the event of a recall. NHTSA does not use the form or the information contained therein for any other reason besides providing consumers with an alternative method of registering their child restraint system.

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).

NHTSA receives information directly from consumers and relies on them to provide accurate information. As NHTSA itself is not using the data for their own purposes, the agency does not verify the information. The agency only collects and forwards the information that has been provided on by the consumer on the form to the appropriate manufacturer. All CRS forms received by NHTSA are sent on to the manufacturer.

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.

NHTSA retains the forms on a secure server encrypted to Federal Information Protection Standard (FIPS) 140-2. The physical (paper) mailed or faxed copies are placed in designated locking disposal bins when information from them has been entered into CRS. The emails that are sent from NHTSA to the manufacturers are encrypted and password protected.

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.

NHTSA is responsible for identifying, training, and holding Agency personnel accountable for adhering to NHTSA privacy and security policies and regulations. NHTSA will follow the Fair Information Practice Principles as best practices for the protection of information associated with the CRS Registration system. Policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. NHTSA manages the risk of collecting the forms by retaining them for a minimal amount of time after forwarding to manufacturers, and does not use the information contained within the form for any other purpose than to provide it to the manufacturers. Forms are stored and sent in adherence with encryption standards.

Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance is also provided in the form of mandatory annual Security awareness training as well as Rules of Behavior. All NHTSA information systems are governed by the NHTSA Rules of Behavior (ROB) for IT Systems. The NHTSA ROB for IT Systems must be read, understood, and signed by each user prior to being authorized to access NHTSA information systems.

The NHTSA Privacy Officer will conduct regular periodic security and privacy compliance reviews consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Cristina Echemendia
General Engineer
Special Vehicle and Systems Division
Office of Rulemaking
1-888-327-4236
www.nhtsa.dot.gov

Approval

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