U.S. Department of Transportation

Privacy Impact Assessment

National Highway Transportation Safety Administration

NHTSA

Corporate Information System (CIF)

Responsible Official

Gopal Rajanala
Director, Office of Information Management
NHTSA
Gopal.Rajanala@dot.gov

Reviewing Official

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

Executive Summary

Pursuant to 49 U.S.C. Chapter 301, the National Highway Traffic Safety Administration's (NHTSA) Office of Defects Investigation (ODI) is responsible for identifying, investigating and ensuring the remedy, through safety recalls conducted by manufacturers, of safety-related defects and non-compliance issues in motor vehicles and items of motor vehicle equipment. To accomplish this, ODI obtains, collects, and evaluates information from several different sources. ODI obtains most its information from consumers and motor vehicle and equipment manufacturers. The remaining information is submitted by State and local law enforcement, insurance companies, automobile dealers, advocacy groups, and other entities. To facilitate internal analytical reporting and statistical analysis of consumer complaints, ODI's investigators and trend analysis staff rely on a centralized suite of analytical applications and data services called the Corporate Information Factory (CIF).

In accordance with Section 208 of the E-Government Act of 2002 a Privacy Impact Assessment (PIA) is required because the CIF system stores Personally Identifiable Information (PII) data on members of the public that is uploaded from the system of record, Advanced Retrieval Tire, Equipment, Motor vehicles Information System (Artemis).

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

[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).

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 CIF is a consolidation of shared data and analytical services. The CIF data services support the administration and program data requirements by federating or integrating source system data near real-time for operational information, and over time for analytical information. All external systems supply datasets for analysis to the CIF via read only connections to a data source or sharing data via extraction saved to a file.

Five DOT systems interact with the CIF by providing data extracts for analysis. These systems are:

- Artemis – Artemis provides an efficient means to identify serious safety defects early in the vehicle equipment and component production cycle and influences safety recalls promoting a safer environment for drivers and passengers across the nation.
- BigFix – Used to report on-demand hardware management services that include asset inventory/discovery, security vulnerability detection and remediation, software distribution, information technology compliance reporting, patch management, software license management, and security policy enforcement.
- Corporate Average Fuel Economy (CAFE) – Used to report fuel Economy performance, manufacturer, financial and civil violation data.
- Cyber Security Assessment and Management (CSAM) – Used to report Plan of Action and Milestone (POA&M) data for different systems.
- Nessus – Used to report computer vulnerability data.

Out of these systems, Artemis is the only one that requires PII data for analytical use within the CIF. Per DOT policy, all CIF related PII data is secured in NHTSA's Enterprise Data Warehouse (EDW), an encrypted database, available for internal use exclusively by the ODI. NHTSA's ODI investigators and trend analysis staff rely on CIF, which is the

Government's enterprise analytical system. The CIF system is a suite of analytical common of the shelf (COTS) applications that are used in the analysis and reporting of data from NHTSA's EDW.

The CIF application provides ODI analysts the ability to visualize complaint and case management data. Investigators use the suite of products to conduct advanced data queries, create visualizations, dashboards, and generate departmental reports.

A subset of the data used for analysis by ODI's investigators contains PII uploaded from the system of record named Artemis.

The uploaded Artemis complaint data elements include:

1. Complainant's name, address telephone number and email
2. Vehicle Identification Number (VIN)
3. Vehicle manufacturer and type (sedan, SUV, van, etc.)
4. Crash details (date, narrative of events) if vehicle was involved in an accident
5. Vehicle complains related or unrelated to accidents

The CIF System is not accessible to the public. Use of the CIF system is exclusive to federal employees and its contractors.

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[2], 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[3].

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

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

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 informs the public that their PII is collected, stored, and used in a number of ways. Through this PIA, published on the DOT website, we identify the purpose of the information collection, NHTSA's authority to collect, store, and use the PII, and all uses of the PII collected, stored, and transmitted. Because the PII data residing in the CIF is updated daily from the Artemis system, any corrections to the PII data should be performed in Artemis. The Artemis PIA identifies the information collection's purpose, use, and storage of PII and can be found at: https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

Records in CIF are not subject to the provisions of the Privacy Act as information is not retrieved by a unique identifier associated with an individual.

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.

NHTSA uses this PIA to inform the public that their PII is stored and used by the system. The CIF is an internal system to NHTSA and therefore not accessible to the public. It receives daily data updates from Artemis to aggregate data, perform analytics, and prepare reports. Once the data in Artemis is modified, the information is updated in the CIF the next day. Because the PII data residing in the CIF is updated daily from the Artemis system, any corrections to the PII data should be performed in Artemis. Individuals can send inquiries regarding privacy concerns or data inaccuracy to NHTSA.Privacy@dot.gov.

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 TREAD Act[4] and 49 U.S.C. Chapter 30166 provide NHTSA with the legal basis for the collection of PII for the purpose of identifying, investigating, and correcting, through safety

[4] The Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act (Public Law 106-414) was enacted on November 1, 2000. This Act includes a requirement that the National Highway Traffic

recalls, safety-related defects in motor vehicles and items of motor vehicle equipment. Specifically, PII is collected for the purpose of contacting consumers regarding vehicle defect complaints they have filed with NHTSA; identifying patterns in other consumer complaint information (vehicle, injury, property damage, alleged defective parts and insurance claim) that indicates a manufacture defect; identifying similar trends in manufacturer quarterly Early Warning Reporting (EWR) information (Make, Model, Year, Fatality Claims and Notices, Injury Claims and Notices. Number of Property Damage Claims, Numbers of Consumer Complaints, Number of Warranty Claims, Number of Field Reports) that indicate a manufacture defect; providing a manufacture with the necessary evidence of the existence of a defect to compel a recall, or if necessary to provide sufficient evidence in a Federal Court to force a manufacturer to issue a recall.

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.

Only the relevant and necessary data elements coming from the Artemis system are required for the purpose of creating analytics for NHTSA employees and contractors. The data elements ensure that the most accurate information is obtained and analyzed to support NHSTA's research and analysis that can further the goals of vehicle safety in the United States. The Artemis data set is refreshed and retained in the CIF database on a daily schedule. Every 24 hours, or on demand, a new data set from Artemis is copied to the CIF, overwriting the PII data from the previous day.

The PII obtained by the CIF system pertains to data elements from the Artemis system required for the purpose of creating analytics by NHTSA employees and contractors. These data elements are refreshed every 24 hours or on demand, they are considered transitory because they have short term value (less than 180 days) and are covered by the NARA's GRS 5.2: Transitory and Intermediary Records item 010[5] (DAA-GRS2017-0003-0001).

Safety Administration (NHTSA) conduct Early Warning Reporting (EWR) rulemaking to require manufacturers of motor vehicles and motor vehicle equipment to submit information, periodically or upon NHTSA's request, that includes claims for deaths and serious injuries, property damage data, communications from customers and others, information on incidents resulting in fatalities or serious injuries from possible defects in vehicles or equipment in the United States or in identical or substantially similar vehicles or equipment in a foreign country, and other information that would assist NHTSA in identifying potential safety-related defects. The intent of this legislation is to provide early warning of such potential safety-related defects.

[5] https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf

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.

NHTSA limits the scope of the PII it collects to data necessary to support the administration of the CIF platform. The CIF uses the collected information about individuals detailed in the Introduction and System Overview section only for the purpose of investigation's case management, operational reporting, and analytics.

NHTSA does not provide information sourced from the CIF system or report to any organization, public or private, unless they have a legitimate need for that information and with which NHTSA has a data sharing agreement, or as required by law.

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 CIF system's data is uploaded and refreshed daily from the system of record, Artemis. When data in the CIF is incorrect, the ODI team makes the proper corrections in the Artemis system. The corrected data appears in the CIF system after the next scheduled or on-demand data refresh from Artemis. The CIF data quality and integrity are thus inherited from the measures taken within the Artemis program.

ODI established quality assurance processes and systems related checks and balances that help preserve the integrity of PII used in support of defect investigations. These include but are not limited to: collecting PII directly from consumers, automated checks in Artemis to ensure completeness and accuracy of reported information, i.e. check sum verification of the Vehicle Identification Number to make sure it's a valid VIN number, files which have undergone the PII redaction process are periodically scanned to validate the effectiveness of the processes, and performing periodic quality assurance reviews of consumer reported information for accuracy and compliance is standard operating procedures.

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.

PII collected and maintained in the CIF is safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. NHTSA security policy and practices are based on NIST Information Risk Management and Security standards. These are supplemented by privacy-specific guidance provided in NIST 800-122 and NIST Special Publication 800-53 Revision 4, and the DOT Privacy Risk Management Policy 1351.18 and the Office of Management and Budget circular A-130, Section 8b(3), Securing Agency Information Systems. The NIST security guides and standards are used by NHTSA to, among other things; assess information confidentiality, integrity and availability risks, identify required security safeguards, and adjust the strength and rigor of those safeguards to reduce risks to appropriate acceptable levels. Under this policy NITSA has implemented appropriate Administrative, Physical and Technical safeguards to protect the confidentiality, availability and integrity of the CIF system and information.

The Corporate Information Factory (CIF) is a FIPs-199 moderate risk system and was granted the authority to operate on November 20th, 2019. Access to the CIF is exclusive to NHTSA employees and its contractors with the appropriate security credentials, PIV card. NHTSA deploys role-based access controls in addition to other protection measures reviewed and certified by the NHTSA's cybersecurity professionals to maintain the confidentiality, integrity, and availability requirements of the system. CIF databases use authentication, authorization, and auditing mechanisms to secure data in the database. To protect data files, the database provides Transparent Data Encryption (TDE), which encrypts sensitive data stored in data files.

The PII data in the CIF system can only be accessed by NHTSA Federal employees and contractors with the proper access to perform analytics and generate reports used within NHTSA. There is no public access to the CIF system.

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 NHTSA employees and contractors accountable for adhering to DOT Privacy and Security policies, and regulations. DOT follows and adheres to Fair Information Practice Principles (FIPPs) for the protection of information associated with the CIF records. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to the protection, retention and disposal of records. NHTSA provides training to employees and contractors on the collection, use, processing and security of the CIF data. The training is mandatory annual security and privacy awareness training. In addition, each NHTSA employee and contractor

with access to the CIF must agree to the system rules of behavior. NHTSA Security and Privacy Officer conduct security and privacy reviews of the CIF consistent with the Office of Management and Budget circular A-130, *Managing Information as a Strategic Resource*, and follow the DOT Privacy Risk Management Policy 1351.18. https://www.transportation.gov/sites/dot.gov/files/docs/CIOP - Privacy Risk Management - 1351.18 - Policy - 09302014.pdf.

Responsible Official

Gopal Rajanala
System Owner
Director, Office of Information Management, NHTSA OCIO

Prepared by: Jose R. Delgado-Forastieri, NHTSA Privacy Officer

Approval and Signature

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer