



U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration
Office Of Defects Investigation

Advanced Retrieval (Tire, Equipment, Motor Vehicle) Information System (ARTEMIS)

Responsible Official

Tanya Topka

Email: tanya.topka@dot.gov

Phone Number: 202-366-4703

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, NHTSA's 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 of 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. ODI uses the Advanced Retrieval (Tire, Equipment, Motor Vehicles) Information System (ARTEMIS) to provide centralized storage, document management and data analysis tools for all information described above. ODI employees and contractors use ARTEMIS in the performance of their day-to-day activities.

As the repository for ODI data, ARTEMIS maintains data from several agency information collections that support ODI's mission. These collections are to support ODI's activities to determine the existence of a safety-related defect in motor vehicles and equipment, or to audit a manufacturer's recall of vehicles or equipment. Except for one collection, the information collections that feed data into ARTEMIS concern information about the motor vehicle or equipment, with potential ancillary information about individuals included in the collection.

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

¹Office 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).



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

Under 49 U.S.C. §§ 30117-30121 and 30166 NHTSA's Office of Defects Investigation (ODI) is responsible for identifying, investigating, and correcting, through safety recalls, safety-related defects in motor vehicles and items of motor vehicle equipment. ARTEMIS is ODI's database system that provides essential defect information collection, cataloging, document management and analysis capabilities that are used in each of these processes.

ODI collects information through several collections and the data is uploaded into ARTEMIS. ODI uses the information in each collection to support its investigation and oversight of motor vehicle and equipment safety defects and noncompliance with Federal Motor Vehicle Safety Standards (FMVSS). The ODI information collections that are included in ARTEMIS are described below.

1. Consumer Complaints

A consumer may submit to NHTSA information related to a safety-related problem and issue with a motor vehicle or an item of motor vehicle equipment. This "consumer complaint" is referred to within NHTSA as a Vehicle Owner Questionnaire (VOQ).

Although the VOQ may be about a motor vehicle, an item of equipment such as a car seat or tire and may include details of a motor vehicle crash, NHTSA has determined that the VOQ information collection is a Privacy Act system of records². This determination is based on

² NHTSA has published a system of records notice (SORN) here: DOT/NHTSA 415 - ARTEMIS System/Vehicle Owner Questionnaire (VOQ) System - 84 FR 17234 - April 24, 2019.



the VOQ including information about individuals and their interactions with motor vehicles or equipment, including crash details.

All VOQ information includes:

- Consumer's Name
- E-Mail Address
- Daytime and Evening Phone²
- Address, City, State, Zip²
- Vehicle Identification Number (VIN)
- Vehicle Make, Model, and Year
- Date of Incident
- Was There Fire (Yes/No)
- Was There Crash (Yes/No)
- Number Of Injuries
- Number Of Deaths
- Was Medical Attention Required (Y/N)
- Vehicle Failed Parts
- Vehicle mileage at time of incident (miles)
- Vehicle speed at time of incident (mph)
- Consumer Narrative³

A complaint may or may not include supporting documentation such as photos, videos, police accident reports, repair invoices or medical information.

Consumer Contact information is necessary to allow NHTSA to contact the consumer to discuss the complaint, and if necessary, collect any additional information that may provide evidence of defect trend. This may include complaints filed with the manufacture, repair estimates, insurance claims and adjuster reports, police accident reports, emergency room and other health care records of specialists providing treatment because of the crash.

A consumer may submit a VOQ to NHTSA though the [NHTSA website](#), NHTSA's mobile SaferCar application called [SaferCar](#), a the "Vehicle Safety Hotline" (a telephone service)⁴, U.S. Mail or Email. Each method of VOQ submission is maintained in ARTEMIS.

Once the VOQ is received, NHTSA assigns it a NHTSA ID Number. NHTSA staff regularly retrieve VOQ data by the by the VIN or its NHTSA ID Number.

NHTSA uses the personally identifying information (PII) in VOQs and consumer letters to contact vehicle owners and lessees whose vehicles are the subject of VOQs, as well as other

³ The VOQ includes a free form text area "Tell Us What Happened" providing the complainant and opportunity to provide additional detail of their incident or complaint. Complainants are advised that because their description may appear in a public NHTSA database, that they should not provide sensitive information through this forum.

⁴ Vehicle Safety Hotline 888-327-4236, Monday-Friday 8am-8pm ET, and Hearing Impaired (TTY): 800-424-9153



individuals referenced in VOQs, to help the Agency identify, investigate and ensure that manufactures remedy, through recall, replacement or repair, (1) potential safety defects and failures to comply with FMVSS in motor vehicles and items of motor vehicle equipment, and (2) problems with the scope, administration, notification or remedy of a recall.

NHTSA also may use the email addresses and VINs collected to notify consumers via email of open recalls applicable to the vehicles or equipment referenced in their VOQs.

Consumers may opt-out of this service when they submit a VOQ. When a VOQ is recorded by NHTSA Hotline personnel, the Hotline agent offers an opportunity to the consumer to opt out of the safety notifications.

While the majority of VOQs submitted to NHTSA are directly from consumers of motor vehicles or equipment, safety advocates, members of Congress, legal representatives, law enforcement, insurance companies and other entities may submit a VOQ on behalf of a consumer or in their own capacity.

Regardless of the method of receipt, each VOQ is assigned a NHTSA ID Number and maintained in ARTEMIS.

2. Early Warning Reporting (EWR)

All motor vehicle and equipment manufacturers are required to submit Early Warning Reporting (EWR) information to NHTSA pursuant to 49 U.S.C. § 30166(m). The type of information submitted and timing of reports depends on the type of manufacturer⁵ and the manufacturer's production level. See 49 CFR part 579, subpart C. Under EWR, manufacturers report information related to 1) motor vehicle and equipment production; 2) information on death and injury claims or notices; 3) aggregate counts of consumer complaints, property damage, warranty claims and field reports by vehicle make, model and model year; and 4) copies of manufacturer field reports. Specifically, these categories include the information elements as follows:

- a. For production data, manufacturers submit the number of vehicles or equipment produced each quarter by vehicle make, model, model year, if applicable.
- b. For death and injury claim data, manufacturers submit the make, model, model year of the vehicle involved, fuel or propulsion system, the VIN, the date of crash, State, and component or system code alleged to contribute to the crash. NHTSA may request additional information related to the crash that may include the police accident report, the claim notifying the manufacturer of the death or injury and the manufacturer's view of the incident.

⁵ The EWR regulation, 49 CFR part 579, sets threshold reporting levels.



- c. For the aggregate counts, the manufacturer reports the count of warranty claims, consumer complaints, property damage claims and field reports received in the quarter by vehicle make, model, model year, and component or system code.
- d. For copies of field reports, the manufacturer provides digital copies (and for some small volume manufacturers, hard copies) of the field reports it receives from its representatives in the field. These reports are about a problem that may be related to a safety defect and may include the VIN.

ODI may request additional records from a manufacturer based upon its EWR submissions through a Comprehensive Inquiry that may include information on individuals such as VIN, injury descriptions, medical records, consumer contact information, other information contained in death and injury claims, and crash related information. Manufacturers may also submit specific consumer complaints, property damage claims, warranty claims, and field reports related to the vehicle or equipment that is the subject of the inquiry.

Manufacturers submit EWR reports to NHTSA through the Manufacturer EWR Portal (MEP) that provides a secure transfer method. The MEP leverages the identity broker Okta to delegate public users to the login.gov identity provider. Once an identity is established, users may submit EWR submissions.

ARTEMIS also includes an interface that connects to NHTSA's website. NHTSA publishes deidentified EWR data on this website for public use.

3. Investigations

Pursuant to 49 U.S.C. § 30166, ODI conducts investigations of potential safety related defects that involve a specific make, model, model year motor vehicle or equipment, component, or system. During an investigation, ODI obtains vehicle or equipment production data from manufacturers, lawsuit information, police crash reports, injury information, warranty claim information, consumer complaint information, design and engineering information, manufacturer communications, and other information that is pertinent to the subject investigation. The information obtained from by the manufacturers may contain information on individuals. For example, warranty claims and consumer complaints may include the name of the individual that submitted the claim, contact information, details related to the claim or complaint, and potential injury information. During the investigation, safety investigators may obtain vehicle crash or defect related information directly from consumers, law enforcement, attorneys, consumer advocates, newspaper articles, journal articles, insurance companies, or other sources of information as is relevant and necessary to further the investigation. ODI investigations are assigned a specific NHTSA action number.



For a manufacturer's submission related to an investigation, ODI employees and contractors regularly retrieve information by the specific NHTSA action number assigned to the investigation number or search by make, model, model year for vehicles and product line, brand name or part number for equipment. ODI employees cannot search the records in an investigation file by an individual's name or an assigned number since the investigation is focused on the specific defect involving the make, model, model year of the vehicle or item of equipment.

4. Foreign Recall Information

Pursuant to 49 U.S.C. § 30166(l), each manufacturer is required to submit by email to ODI information on recalls conducted in foreign countries that is identical or substantially similar to a vehicle, item of equipment, or tire sold or offered for sale in the United States. The manufacturer must provide:

- the name of the submitter
- make, model, model year of the vehicle
- number of vehicles involved in the recall

5. Domestic Recall Information

Pursuant to 49 U.S.C. §§ 30118, 30119 and 49 CFR parts 573 and 577 manufacturers are required to notify NHTSA of a safety related defect or noncompliance with a FMVSS. This notice must include the make, model, model year of the vehicle or equipment, the component or system involved, the number of vehicles or items of equipment, a VIN range of the affected vehicles, a description of the defect or noncompliance, a chronology of events leading to the discovery of the defect or noncompliance, a remedy plan, copies of communications or service bulletins related to the defect or noncompliance, and a draft notice to consumers informing them of the recall. Manufacturers are also required to submit quarterly progress data identifying the percentage of vehicles or equipment subject to the recall that have been remedied. Recalls are assigned a specific NHTSA Campaign number.

6. Manufacturer Communications

Pursuant to 49 U.S.C. § 30166(f), on a monthly basis, each manufacturer is required to submit to ODI a copy of all notices, bulletins and other communications sent to more than one manufacturer, distributor, dealer, lessor, lessee, owner, or purchaser in the United States regarding any defect in its vehicles or items of equipment. The information included in these communications contain vehicle type, details regarding the alleged defect, remedy details and other information pertinent to the vehicle or repair that is the subject of the communication.

7. SaferCar App



In addition to the ability for consumers to submit a VOQ, the SaferCar app provides users with the ability to search, browse, and save their products (vehicles, car seats, tires, and equipment) to a user dashboard on their cellphones. All SaferCar app data submitted or retrieved by the individual remains only in the app on the individual's cellphone. When a user saves a product to his or her device dashboard, the app will check for new safety information related to any saved products and notify the individual of the availability of new safety information and recalls. No external systems are needed for storing the information provided to the app.

8. Standing General Order (SGO)

On June 29, 2021, NHTSA issued a Standing General Order 2021-01⁶ (SGO) to motor vehicle manufactures and operators of certain Advanced Driver Assistance Systems (ADAS) and Automated Driving Systems (ADS). The SGO requires manufacturers and operators of vehicles equipped these systems to report crash incidents of such vehicles. The data reported includes the subject vehicle information, incident information, incident scene, crash description, post-crash information and a narrative that allows the reporting entity to provide details of the incident, such as whether the ADAS/ADS feature engaged prior to and during the incident.

To meet the requirements of the SGO, a manufacturer or operator point of contact must log in to NHTSA's web based SGO portal and submit the following information about each applicable crash:

- Subject Vehicle
 - Vehicle Identification Number (VIN)
 - Vehicle Serial Number
 - Vehicle Make, Model, and Year
- Incident Information
 - Incident Date and Time
 - Incident location
 - Address, City, State and Zip
 - Latitude and longitude

9. First Responder Incident Advanced Reporting (FRIAR)

The First Responder Incident Advanced Reporting (FRIAR) is a collection that permits first responders to report motor vehicle or equipment safety issues to NHTSA. The FRIAR collection supports the DOT safety strategic goal by collecting information from first responders about suspicious and urgent motor vehicle and equipment safety matters.

If a first responder believes that an injury or death occurred due to an alleged or suspected safety defect, the first responder may submit information to NHTSA to provide basic

⁶ [Standing General Order 2021-01, Second Amended \(nhtsa.gov\)](https://www.nhtsa.gov/standards-requirements-and-guidance/safety-criteria/standing-general-order-2021-01).



information concerning the incident that NHTSA can review to determine whether further review is necessary.

The PII elements included in FRIAR include:

- Vehicle Identification Number (VIN)
- Date and location of the incident
- A short summary of what occurred
- First Responder point of contact information

Even when is not required, first responders have the option to upload supporting documents, pictures, etc. These documents may or may not contain information about the individuals involved in the accident and EMS records.

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) v3⁷, 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 Organizations⁸.

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 informs the public that their PII is collected, stored, and used in several ways. Through this Privacy Impact Assessment, published on the DOT website, we identify the information collection's purpose, NHTSA authority to collect, store, and use the PII, and all uses of the PII collected, stored, and transmitted through the ARTEMIS system. The SaferCar website and Mobile Application contain a link to the DOT Website Privacy Policy which outlines our online information practices, <http://www.nhtsa.gov/Privacy>. The

⁷ <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

⁸ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf



consumer complaints website, <https://www.nhtsa.gov/report-a-safety-problem#index> also includes specific reference to the system of records notice (SORN) [DOT/NHTSA 415 - ARTEMIS System/Vehicle Owner Questionnaire \(VOQ\) System - 84 FR 17234 - April 24, 2019](#) designating the VOQ portion of ARTEMIS as a Privacy Act system of records.

In addition to the VOQ SORN, NHTSA published notices of an information collection for multiple information collections that are maintained in ARTEMIS. These OMB Information Collection Requests (ICR) and other regulations include:

- | | |
|---|--|
| 1. Vehicle Owner Questionnaire (VOQ) | ICR#: 2127-0008 |
| 2. Early Warning Reporting (EWR) | ICR#: 2127-0616 |
| 3. Defect Reports (Part 573 and Part 577) | ICR#: 2127-0004 |
| 4. Potential Defect Retention (Part 579) | ICR#: 2127-0616 |
| 5. Standing General Order 2021-01 (SGO) | Standing General Order 2021-01, Second Amended (nhtsa.gov) |

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.

Consumers filing complaints may request a correction to complaint information by contacting NHTSA through its Hotline number at 888-327-4236.

Changes to PII received from motor vehicle manufacturers, insurance companies, and other public and private entities are permitted, but only by the entity that originally promulgated the document. This is required to preserve the integrity of NHTSA's investigation information.

Privacy Act requests for access to an individual's record must be in writing (either handwritten or typed). DOT regulations require that the request include a description of the records sought, the requester's full name, current address, and other relevant contact information. The request must be signed and either notarized or submitted under penalty of perjury. Privacy Act requests concerning Artemis information may be addressed to:

U.S. Department of Transportation (DOT)
National Highway Traffic Safety Administration (NHTSA)
Director of Office of Defects Investigations (NEF-010) West Building
1200 New Jersey Ave, SE
Washington, DC 20590



Consumers with concerns about any data privacy or accuracy matter are encouraged to contact the NHTSA Privacy Officer at any time at the following email address:

NHTSA.Privacy@Dot.Gov.

Additional information and guidance regarding the Freedom of Information Act and Privacy Act program may be found on the [FOIA | NHTSA](#) website.

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.

49 U.S.C. §§ 30117-30121 and 30166 provides NHTSA with the legal basis for the information collections that contain PII. These authorities authorize NHTSA to collect this information for the purpose of identifying, investigating and correcting, through safety recalls, safety-related defects in motor vehicles and items of motor vehicle equipment. Each collection is collected for a specific role to assist NHTSA in its statutory authority. For example, NHTSA collects VOQs to learn of concerns in the field and to contact those consumers who submit a complaint to follow-up or learn more about a specific complaint. Other collections, such as EWR data, (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) provide NHTSA with information from manufacturers that may assist in the early identification of a safety related defect. Information collected pursuant to an investigation may support ODI to NHTSA's ability to identify patterns in information (vehicle, injury, property damage, alleged defective parts and insurance claim) that indicates a safety defect. Foreign recall information supports NHTSA in identifying similar vehicles in the United States that potentially have a safety related defect. All the data collected by ODI and maintained in ARTEMIS may be used as evidence to support the agency's enforcement through legal action to compel a manufacturer to conduct a safety related 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.

NHTSA's Office of Defects Investigation (ODI) collects, uses, and retains in the ARTEMIS system only the data elements that are relevant and necessary for the purposes of 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. For example, while manufacturers are required to submit EWR



information related to death and injuries, NHTSA does not compel information about an individual that was killed or injured in a motor vehicle crash.

NHTSA maintains records in ARTEMIS under an approved National Archives and Records Administration (NARA) record schedule. The NARA identifier for these records is NHTSA's Office of Defects Investigation (ODI), DAA-0416-2019-0003⁹.

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 use of the information it collects and stores in ARTEMIS to its statutory purpose of identifying, investigating, and correcting, through safety recalls, safety-related defects in motor vehicles and items of motor vehicle equipment. Accordingly, ODI uses the records in ARTEMIS to identify trends that could result in defect investigations, and ultimately in safety-related recalls. ODI may use each information collection individually or collective to support its mission to identify safety related defects and ensure that manufacturers take the appropriate steps to remedy safety related defects or noncompliance with a Federal Motor Vehicle Safety Standard.

For the overwhelming majority of the PII in ARTEMIS, NHTSA does not share it publicly, subject to Federal law. Prior to disclosure, NHTSA redacts PII from ARTEMIS records. NHTSA will not sell or lease any PII. NHTSA permits external sharing of PII only for a purpose compatible with the original purpose of the collection, as authorized by Federal law. For example, ODI may share complaints about safety defects or recall performance to manufacturers to allow them to research the root cause and, if necessary, rectify owner complaints and problems; to refer complaints to the appropriate State or Federal agency for actions involving matters of law or regulation beyond the responsibility of the agency or Department, such as the Federal Trade Commission in matters involving warranties. NHTSA has published these uses in its system of records notice for the VOQ information collection. See <https://www.govinfo.gov/content/pkg/FR-2019-04-24/pdf/2019-08171.pdf>.

⁹ https://www.archives.gov/records-mgmt/rcs/schedules/departments/departments-of-transportation/rg-0416/daa-0416-2019-0003_sf115.pdf



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 information submitted to ODI is typically directly from individuals who submit a complaint, someone on their behalf, or from motor vehicle or equipment manufacturers. NHTSA assumes that the PII submitted by individuals is accurate since the individual is supplying NHTSA with the information. NHTSA does not control the collection of information by manufacturers that is ultimately submitted to NHTSA. NHTSA relies on the accuracy of the PII provided to it by manufacturers. As part of its investigation process, if NHTSA learns of inaccurate PII in information provided to it by a manufacturer, it corrects the record in its files.

ODI has established quality assurance processes and systems related checks and balances that help preserve the integrity of PII used in support of safety related defect investigation and remedy of safety recalls.

To improve the quality during the data collection and preventing errors as the information is collected, some of the collected PII comes directly from the consumers, and the ODI investigators also double checks the collected data when interviewing individuals during the investigations.

To minimize mistakes during the data entry process, the system does an automatic data validation to verify the data types of the collected information (numbers, dates and text) are entered correctly in their own respective data fields, and the VIN performs a check sum verification to confirm it is a valid VIN.

ODI also deletes PII from the data fields where the PII should not be entered, like general description fields.

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.

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. 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, NHTSA has implemented appropriate administrative, physical, and technical safeguards to protect the confidentiality, availability and integrity of the ARTEMIS system and information. All federal employees and contractors undergo appropriate background checks prior to being granted access to the DOT systems. In addition, all ARTEMIS users receive both general and role-based security training on an annual basis. ARTEMIS utilizes role-based security to restrict user access to application functions and information required to fulfill their job function. ARTEMIS enforces assigned authorizations for controlling access to the system using unique username/password combinations and roles and group membership. The ARTEMIS application maintains an audit trail of changes made, date/time of change, and the username for each database change.

All remote network communications are encrypted using Federal Information Processing Standard (FIPS)-140 certified encryption modules. Remote access to ARTEMIS IT Infrastructure is provided via the DOT Secure Remote Access solution. By policy and design, direct access to ARTEMIS from public networks is not allowed.

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 ARTEMIS 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 ARTEMIS data. The training is mandatory annual security and privacy awareness training. In addition, each NHTSA employee and contractor with access to ARTEMIS must agree to the system rules of behavior. NHTSA Security and Privacy Officers conduct security and privacy reviews of ARTEMIS consistent with the Office of Management and Budget circular A-130, Section 8b(3), Securing Agency Information Systems and follow the DOT Privacy Risk Management Policy 1351.18. - https://www.transportation.gov/sites/dot.gov/files/docs/dotorders/DOT1351.18_Privacy%20Risk%20Management_30-Sep-14.pdf.



Responsible Official

Tanya Topka
System Owner
Office Director, Office of Defects Investigation

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

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

DOT CPO Adjudicated 04/29/2024