U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration (NHTSA)

Motor Vehicle Importation Information System (MVII)

Responsible Official

Jeff Giuseppe
Associate Administrator
Enforcement (NEF-010)
202-366-5756
Jeff.Giuseppe@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
Date: 2018.12.19 21:19:19 -05'00'

Executive Summary

Pursuant to Title 49 of the U.S. Code, Chapter 301 Motor Vehicle Safety, the National Highway Traffic Safety Administration (NHTSA) has authority to carry out motor vehicle and highway safety programs. Under its statutory authority, NHTSA establishes and enforces Federal Motor Vehicle Safety Standards (FMVSSs). To manage and analyze the data associated with vehicle importation and safety compliance, NHTSA developed the Motor Vehicle Importation Information (MVII) system. This system maintains vehicle importation and compliance process information, Registered Importer (RI) identification, and vehicle petition information.

A Privacy Impact Assessment (PIA) is required as MVII contains personally identifiable information (PII) on members of the public. The previous PIA was published January 23, 2004. This update is being conducted to ensure the PIA accurately reflects the current system.

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

NHTSA's Office of Vehicle Safety Compliance (OVSC) enforces the requirement that all motor vehicles and equipment manufactured or imported for sale in the United States meet all applicable FMVSSs[1]. Motor vehicles and items of regulated motor vehicle equipment are considered "conforming" if they are covered by a manufacturer's certification that they meet all applicable FMVSS. Conforming vehicles and equipment may be imported into the U.S. free of restriction. A nonconforming vehicle may be imported on a permanent basis only if NHTSA deems it eligible for importation, based on its capability of being modified to conform to all applicable FMVSSs.

NHTSA makes import eligibility decisions based on petitions filed by registered importers (RIs). RIs are NHTSA-licensed commercial entities who are permitted to import nonconforming vehicles and bring them into compliance with all applicable FMVSS. If NHTSA decides, by granting a petition for import eligibility, that a vehicle of a particular make, model, and model year is eligible for importation, the vehicle may be imported only by an RI or by a person who has a contract with an RI to modify the vehicle so that it complies with all applicable FMVSSs following importation. The system that is used to monitor the importation of motor vehicles and motor vehicle equipment is MVII. MVII is primarily used as a tracking system to monitor the importation of noncomplying motor vehicles imported by RIs. Information is also recorded about RIs, importation related petitions, the duration of RI vehicle processing and associated fees.

NHTSA requires the importer of a motor vehicle or item of motor vehicle equipment to file a declaration with the U.S. Customs and Border protection (CBP) setting forth the lawful basis for the item's entry into the United States. This declaration is made on the DOT HS-7 form (OMB No. 2127-0002). The HS-7 Declaration form contains 14 boxes, each of which sets forth a lawful basis for the importation of a motor vehicle or motor via equipment. The declaration may be filed in hard copy or electronic form.

Electronic Submission of Form HS-7

To file electronically, data is entered into the CBP's Automated Broker Interface (ABI) system by a Customs House Broker hired by the importer. The agency has statutory authority and OMB approval to collect he information that is transmitted. The information collected electronically from CBP ABI system includes: the importer's identification number (if the importer is registered with NHTSA, this would be a five-digit code assigned by the agency), name, address, vehicle identification number (VIN), any equipment information, surety information, and the names, street address, city, state, zip code and sometimes signature of the owners of the vehicles or equipment being imported. Occasionally, files received from customs list a Tax Identification Number (TIN) or social security number of an individual seeking to import his or her own vehicle into the U.S. in place of the importer's identification number. In these cases, which are rare, there is no way for most OVSC staff to tell whether the number appearing in the "identification number" field is a TIN, SSN, or other number, as this information is entered into the ABI system by the customs broker, and is not transmitted to NHTSA with any unique or distinguishing designation identifying it as anything other than an "identification number."

Once the data is entered into CBP's ABI, it is transmitted to NHTSA via the ACE/ITDS system. DOT has a Memorandum of Understanding (MOU) with CBP that permits the transmission of the data to NHTSA. When NHTSA receives the information from CBP, it is uploaded it to the agency's MVII database, which houses information on motor vehicles and equipment imported into the United States. This allows the importer to bring the vehicle into

[1] 49 U.S.C. § 30112(a)(1)

the U.S. for modification. After performing modifications to bring the vehicle into compliance with all applicable FMVSS, the RI submits a statement of conformity to NHTSA. If the agency is satisfied that all necessary modifications have been made to the vehicle, it will issue a letter to the RI releasing the DOT conformance bond that was furnished at the time of entry and close its electronic record of the vehicle.

In addition to conforming and nonconforming vehicles imported in the manner described above, declarations are filed for nonconforming vehicles that are temporarily imported by nonresidents or foreign diplomats or military personnel for personal use, or by other individuals and entities for purposes of investigations, research, demonstrations or training, or competitive racing events. Declarations are also filed for vehicles imported in a limited number of other circumstances, all specified on the HS-7 Declaration form.

OVSC staff members have access to importer identification numbers for work-related purposes. Importer identification numbers may be needed by these OVSC staff members because of compliance investigations.

New data is batch uploaded into the MVII system from Customs and Border Protection (CBP) importation data files from the CBP ABI system. This data is saved on NHTSA servers. MVII can generate and tracking official Office of Vehicle Safety Compliance (OVSC) correspondence, generating reports that identify the fees incurred by RIs, and generating other reports containing data related to the importation of motor vehicles and motor vehicle equipment.

Submssion of Hardcopy Form HS-7

Occasionally, CBP also sends NHTSA hard copies of HS-7 forms filed by customs brokers or importers via express or U.S. mail. Additionally, RIs file hard copies of paperwork containing HS-7 and other forms such as vehicle or business (belonging to either the RI or their customer) directly with NHTSA. NHTSA staff manually enters this information into the MVII system for processing. Instead of entering into MVII, NHTSA processes the hard copies of HS-7 forms received from Customs CBP and RI-filed paperwork containing HS-7 forms under certain product categories, such as 2A (certified vehicle) and 8 (non-motor vehicle) and stores them in a secure file room. In addition to the processes detailed above, MVII generates correspondence and reports that assist OVSC in enforcing Federal importation laws and regulations.

At the time of importation, most vehicles have yet to be sold to their first purchaser in the United States. For this reason, most of the VINs referenced on H-7 forms relate to a commercial entity and not an individual. However, as noted on the H-7 form itself, there are some occasions, albeit rare, when nonresidents or foreign diplomats or military personnel, or other individuals or entities (e.g., a sole proprietorship or “DBA”) U.S. citizens, Military and Civilian employees, nonresidents seek to import conforming or nonconforming vehicles. In such cases, the name, address, city, state, zip code, signature, VIN, and sometimes social security number, country of origin, and/or passport number for that individual are listed on the HS-7. In such cases, Official Orders issued by a foreign government or embassy may be attached to the HS-7. However, the vast majority of the information collected, used, retained and generated by the MVII system is commercial in nature, as RIs, typically, are commercial entities and most vehicles imported through the processes detailed above are owned by car manufacturers and dealers.

In addition to the PII that may be obtained from HS-7 forms, MVII collects and maintains PII of federal contractors and employees who require access to the system. This information includes name and login information.

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 provides notice of the information it requires from individuals who wish to import a vehicle on its Vehicle Importation and Certification Webpage: https://icsw.nhtsa.gov/cars/rules/import/

As required by the Privacy Act, DOT/NHTSA provides direct notice to individuals via Privacy Act Statements on all paper and electronic forms it uses to collect PII that is subject to the Act. Notice is also provided to individuals through the Privacy Act System of Records Notice (SORN) DOT/NHTSA 463 – Motor Vehicle and Motor Vehicle Equipment Import - 65 FR 19550 - April 11, 2000.

Additionally, NHTSA uses this Privacy Impact Assessment (PIA) to inform the public that their PII is stored and used ny the system. The PIA identifies purpose for which the PII collected. It can be found 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.

NHTSA ensures that individuals have the right to (a) obtain confirmation of whether NHTSA has PII relating to them; (b) access the PII related to them within a reasonable time, cost, and manner and in a form that is readily intelligible to the individual; (c) obtain an explanation if such a request is denied and be given the opportunity to challenge such denial; and (d) challenge PII relating to him or her, and if the challenge is successful, have the data erased, rectified, completed, or amended. Privacy Act requests for access to an individual's record must be in writing, but it may be mailed, faxed or emailed.

Individuals seeking access or contesting information about them in the MVII can make a request in writing to the NHTSA Privacy Office located at the Department of Transportation 1200 New Jersey Avenue, SE Washington, DC 20590. The request must include the requester's name, mailing address, telephone number, and/or email address;

a description and the location of the records requested. When seeking records about yourself from this system of records, your request must conform to the Privacy Act regulations set forth in 49 CFR part 10. You must verify your identity by: (1) Having your signature on your request letter witnessed by a notary; or (2) including the following statement immediately above the signature on your request letter: "I declare under penalty of perjury that the foregoing is true and correct. Executed on [date]." If you request information about yourself and do not follow one of these procedures, your request cannot be processed.

Additionally, an individual can contact a responsible NHTSA staff member to address a privacy concern or data inaccuracy or 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 its collects, uses, maintains, or disseminates PII.

Pursuant to Title 49 of the U.S. Code, Chapter 301 Motor Vehicle Safety, the National Highway Traffic Safety Administration (NHTSA) has authority to carry out motor vehicle and highway safety programs. Under its statutory authority, NHTSA establishes and enforces Federal Motor Vehicle Safety Standards (FMVSSs) which are implemented by 49 CFR Part 591.

MVII collects PII to manage the motor vehicle importation process, ensuring that motor vehicles that were not originally manufactured to comply with all applicable FMVSS are lawfully imported. MVII stores records related to permanent and temporary importation of nonconforming motor vehicles. These vehicles may be imported permanently by an RI, or a person who has a contract with an RI to bring the vehicle into compliance with applicable FMVSS. Alternatively, vehicles may be imported temporarily, such as those imported by foreign military, nonresidents of the United States, or imported for the purposes of research, investigations, demonstration or training, or competitive racing events. NHTSA also uses MVII to enforce its regulations that prohibit importers from entering salvage, repaired salvage, or reconstructed motor vehicles.

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 collects, uses, and retains in MVII only the data elements that are relevant and necessary for the purposes of enforcing statutes and regulations related to the importation of motor vehicles and regulated motor vehicle equipment.

NHTSA has requested a retention period of 5 years for all records maintained in MVII. This retention period aligns with the CBP statute of limitations for records in ACE/ITDS . The paper files are stored for one year in locked file cabinets at the NHTSA DOT Headquarters facility and then shipped for secure storage at a National Archives and Records Administration (NARA) facility.

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.

MVII access is restricted to Federal employees and contractors through a password-protected application loaded on agency computers housed in the DOT headquarters building. There is no public access to the MVII system.

NHTSA receives requests for MVII information from individuals (such as prospective vehicle purchasers), business entities (such as car dealers, car auctions, and RIs) organizations (such as trade associations). The agency provides non-PII MVII data after verifying the requestor's identity and the requestor's need for the information. NHTSA also receives request from other government agencies (both State and Federal) that have a legitimate need for that information and with which NHTSA has data sharing agreements.

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 collects data in electronic format related to imported vehicles. Before the data is imported into the MVII database, several data integrity and validation checks are performed. Contractors compare existing and new data to find missing, inaccurate, or duplicate entries. The agency may request changes to the CBP data and validate entry data with the importer. Customs House Brokers who made erroneous entries into the ABI system may also request that MVII data be amended by submitting written requests or updated Customs Release forms via postal mail (NHTSA, Office of Vehicle Safety Compliance, Import and Certification Division, 1200 New Jersey Ave., SE, WEF-230, Washington, DC 20590), or via email to importcertification@dot.gov. MVII contractors do not delete or void records unless exact duplicates are found.

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 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 MVII system and information. All federal employees and contractors undergo appropriate background checks prior to being granted access to the DOT network. In addition, all MVII users receive both general and role-based security training on an annual basis.

MVII utilizes role-based security to restrict user access to application functions and information required to fulfill their job function. MVII enforces assigned authorizations for controlling access to the system using unique username/password combinations and roles and group membership. The MVII 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 MVII IT Infrastructure is provided via the DOT Secure Remote Access solution. By policy and design we do not allow direct access to MVII from public networks.

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 the organization's personnel accountable for adhering to the DOT and NHTSA privacy and security policies and regulations. NHTSA follows the Fair Information Principles as best practices for the protection of PII. The current practices, policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual privacy awareness training. The NHTSA Security Officer and Privacy Officer conduct regular periodic security and privacy compliance reviews of the Data Repository consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Jeff Giuseppe
Associate Administrator
Enforcement
Jeff.giuseppe@dot.gov

Approval

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