U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration (NHTSA)

National Driver Register (NDR)

Problem Driver Pointer System (PDPS)

Responsible Official

Frank Subalusky
Chief
National Driver Register (NDR)
(888) 851-0436
NDR_Info@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: 2019.03.03 19:16:36 -05'00'

Executive Summary

Title 49 of U.S. Code, Chapter 303, § 30302, requires that the Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) establish and maintain a National Driver Register (NDR). The purpose of the NDR is to assist chief driver licensing officials of all 50 states and the District of Columbia (D.C.) (hereafter referred to as "Jurisdictions") in exchanging information about the motor vehicle driving records of individuals. NHTSA developed Problem Driver Pointer System (PDPS) system, to provide a centralized repository of information on individuals whose privilege to operate a motor vehicle have been revoked, suspended, cancelled, denied, or who have been convicted of serious traffic-related offenses. Licensing officials are required to submit information to PDPS. Any time a person applies for a new driver's license or the renewal of an existing license, the Jurisdiction's driver licensing officials search PDPS to determine if the license or privilege to drive a motor vehicle has been withdrawn. Allowing Jurisdictions to identify problem drivers prior to licensing supports NHTSA's mission to ensure the safety of the general driving public.

A Privacy Impact Assessment (PIA) is required for PDPS, as it contains personally identifiable information (PII) on members of the public. The previous PIA was published November 17, 2003. NHTSA updated this document because PDPS was modernized from a main-frame environment to a client server architecture. DOT and NHTSA also wish to provide greater transparency to the public regarding the system operations.

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 Problem Driver Pointer System (PDPS) is a computerized database owned and operated by the NHTSA NDR. PDPS provides information on individuals whose privilege to drive have been revoked, suspended, cancelled, denied, or who have been convicted of serious traffic-related offenses. The Chief Driver Licensing Official of a Jurisdiction (i.e., the state's or other Jurisdiction's Department of Motor Vehicles (DMV)) is required to send information on all revocations, suspensions, and denied licenses to PDPS. Jurisdictions must also conduct a PDPS search as part of Federal requirements to determine if the license or privilege to drive a motor vehicle has been withdrawn when issuing new or renewed driver licenses.

Personally Identifiable Information (PII) and NDR

The records maintained in PDPS consist of problem driver identification information, including full legal name, date of birth (DOB), sex, and driver license number (DLN) and suspension or revocation status of drivers about whom a Jurisdiction has a driver record.

Full legal name and DOB are used for performing a search on an individual on PDPS. Jurisdictions of Record may send additional identifying information to the PDPS such as aliases, social security number (SSN), height, weight, sex and eye color. Title 49 of U.S. Code, Chapter 30304(b) requires reports from Jurisdictions of Record to contain SSN if it used by the Jurisdiction of Inquiry for driver record or licensing purposes, and the operator license number is different from the SSN. Many Jurisdictions use SSN to help determine driver license eligibility. This includes helping to resolve issues of identification among drivers with common names and shared dates of birth.

Transmission/Submission of Data to PDPS from Jurisdictions

Jurisdictions of Inquiry submit data to PDPS through the secure American Association of Motor Vehicle Administrators network (AAMVAnet). All messages are sent in a standard format in order to simplify the processing of queries. The Jurisdiction's system passes the message through the AAMVAnet, which determines the intended recipient system. If PDPS is the intended system, AAMVAnet sends the encrypted message to PDPS for processing. After the message is processed by PDPS, PDPS will send a response, through AAMVAnet back to the Jurisdiction of Inquiry that submitted the request regarding whether there is suspension or revocation.

Query of Data

When Jurisdictions of Inquiry perform a search on an individual, they submit the individual's full legal name and date of birth to PDPS. PDPS will then search for the individual. If a record is identified, PDPS will "point" the Jurisdiction of Inquiry to the Jurisdiction of Record, where an individual's driver status and licensing history are maintained.

Return of Data to Jurisdiction

Once a user is pointed to the Jurisdiction of Record, the PDPS system will provide one of the following messages in response to the request:

- **"No Match":** No record found for the individual in PDPS.
- **"Match":** Record found in PDPS.

In addition to the "Match" PDPS will also provide the following status information about the individual:

- **"LIC" (Licensed):** Licensed means the individual holds a license and the privilege to drive is valid. (Only drivers who previously had a suspension/revocation and have cleared their history are included here.)
- **"ELG" (Eligible):** The individual's privilege to apply for a license is valid.
- **"NOT" (Not Eligible):** The individual's privilege to drive is invalid.
- **"RPD" (Reported Deceased):** Driver has been reported deceased.

Search results may include multiple probable matches. If there is a match,the minimal result will include first name, last name, and DOB. However, it is possible that SSN, and hair and eye color are are included in the result. PDPS only queries for first and last name, and DOB, but certain Jurisdictions of Record include more data when they submit information to PDPS. That information will be returned as a result of the query.

Use of Data

It is the responsibility of the Jurisdiction of Inquiry to verify and make licensing decisions based on the information they receive from PDPS. Once the data is returned, NDR and NHTSA have completed their part in the process and do not use the information for any reason.

Other Users and Queries – Federal Entities

In addition to Jurisdictions, PDPS information is available to statutorily-authorized users under 49 U.S.C. 30305 (e.g., Federal and non-Federal employers or prospective employers of motor vehicle operators, Federal Aviation Administration (FAA) for airman medical certification, employers of locomotive operators, United States Coast Guard (USCG) for merchant mariners and servicemen, air carriers for pilot applicants, National Transportation Safety Board (NTSB), Federal Highway Administration (FHWA), and Federal Motor Carrier Safety Administration (FMCSA)). These authorized federal agencies have a direct connection to PDPS. They submit a batch inquiry file via SFTP and PDPS processes the file after-hours. The results can be retrieved by these agencies the next day. Although the query process is the same, these agencies' uses of PDPS differ depending on the agency.

Other authorized Federal agencies (ex. NTSB) can contact NDR directly to initiate a PDPS search and NDR will provide them with the results back. These Federal agencies also have the option to submit a request for a PDPS search through a Jurisdiction's DMV on their behalf.

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.

It is the sole responsibility of Jurisdictions of Record to provide notice to individuals that their records have been entered into the system. Neither DOT nor NHTSA enter driver information in PDPS, and cannot provide notice to individuals that their record is included in the PDPS system. However, under the Privacy Act, individuals are authorized to request information from the NDR, which is covered under the Privacy Act System of Records (SORN) for DOT/NHTSA 417 – National Driver Register.[1]

NHTSA maintains a public website which includes the most up to date information on NDR and the PDPS.[2] Additionally, the program's PIA and SORN may be found on the DOT Privacy Program's website.[3]

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.

It is the responsibility of the Jurisdiction of Record to provide notice to the individual of how to access, amend or delete information about her or him from PDPS. For an individual's PII to be sent to PDPS by a Jurisdiction of Record, that individual's driving privilege must have been revoked, suspended, cancelled, or denied; or the individual must be convicted of one or more serious traffic-related offenses. As each Jurisdiction of Record is responsible for identifying problem drivers, each Jurisdiction of Record's procedures determine whether individuals are notified that their PII is sent to PDPS.

Because Jurisdictions of Record maintain the actual driver history data that forms the basis for indentification to PDPS, individuals must contact the reporting Jurisdictions of Record directly to request changes and information. If an individual has been misidentified, for example, the Jurisdiction of Record must notify NDR to correct the information in PDPS. The NHTSA website includes a list of Jurisdictions of Record's DMV addresses and phone numbers that individuals may contact for more information on resolving these issues. NDR staff may assist individuals and help facilitate problem resolution with participating Jurisdictions of Record. For general questions, individuals can contact NDR by calling Monday through Friday, excluding Federal holidays, from 8:30am to 5:00pm EST Toll-free: (888) 851-0436 and/or emailing NDR_Info@dot.gov .

Under the provisions of the Privacy Act, individuals may request access to their records that are maintained in a system of records in the possession or under the control of DOT by complying with DOT Privacy Act regulations,

[1] See 65 FR 19548, April 11, 2000, https://www.gpo.gov/fdsys/pkg/FR-2000-04-11/pdf/00-8505.pdf#page=73
[2] The NDR website may be found at https://www.nhtsa.gov/research-data/national-driver-register-ndr. -
[3] See https://www.transportation.gov/privacy

49 CFR Part 10 (as noted in 23 CFR § 1327.6(j)(3)). As stated above, Privacy Act requests must be in writing and notarized. The request must include full legal name and date of birth.

The request must be mailed to:

National Driver Register
1200 New Jersey Avenue, S.E., NSA-220,
Washington, DC 20590

Additional information and guidance regarding DOT's FOIA/PAprogram may be found on the DOT website. Privacy Act requests also may be addressed to:

Claire W. Barrett
1200 New Jersey Ave., SE E31-312
Washington, DC 20590
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.

NHTSA's NDR is maintained in accordance with Title 49 of U.S. Code, Chapter 303.

PDPS collects PII in order to provide Jurisdictions of Inquiry's Departments of Motor Vehicles (DMV)and other authorized users with information on problem drivers. Jurisdiction of Inquiry's DMVs use this information to make driver licensing decisions, and other authorized users use this information for statutorily-specified purposes such as employment considerations for motor vehicle drivers, railroad operators and pilots; airmen's certificate determinations; and accident investigation, etc. per 49 U.S.C. § 30305.

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.

PDPS collects the information required to allow participating Jurisdictions of Inquiry to make informed driver licensing decisions. Jurisdictions of Record may provide additional information, including SSN, to PDPS. This information will be used to narrow down search results under the system. NDR ensures that the collection, use and maintenance of information collected for operating the PDPS is relevant to the purposes for which it was collected, and to the extent necessary for those purposes; that it is accurate, complete, and up-to-date. The mandatory data (name and date of birth) are the minimum required to perform a search. However, additional data may be sent by the Jurisdiction of Record. These additional data are optional, but useful for helping the Jurisdiction of Inquiry make appropriate licensing decisions.

The substantive records for the PDPS are held in accordance with the following schedules: 1) Master file records are deleted/destroyed when no longer needed for administrative, legal, audit, or other operational purposes, 2) Probable match identifications are deleted/destroyed 7 years after date of disclosure. In general, the Jurisdictions of

Record are responsible for maintaining the records on PDPS. A record will be removed from the file when: 1) The Jurisdiction of Record no longer considers the individual a problem driver, 2) The Jurisdiction of Record's record retention policy requires removal, 3) The Jurisdiction of Record can no longer produce history supporting the record, or 4) The Jurisdiction of Record's record does not the meet the Federal requirements for identifying a problem driver. When the Jurisdiction of Record is unable to delete their pointer record, NDR may delete a PDPS record at their request. NDR will track and document this request. Records that have been disclosed as the result of an inquiry are retained by the NDR for seven years.

NHTSA is in the process of aligning the retention periods expressed in the National Driver Registry System of Records Notice and NHTSA Records Control Schedule with the ones found herein.

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.

PDPS allows Jurisdictions to identify drivers who have had their licenses withdrawn, suspended, revoked or otherwise denied for cause, or who have been convicted of certain traffic violations. This identification is in response to inquiries from jurisdictional or Federal driver's licensing officials. The information in PDPS is used by the Jurisdiction of Inquiry for the express purpose of identifying these problem drivers in the databases of other Jurisdications. The staff at NDR does not access PDPS records unless the Jurisdiction of Record requests help to delete a pointer record, and/or a notarized Privacy Act request is mailed from the subject of the record or his or her representative. NHTSA does not use the information in any other manner other than allowed by Federal regulation and described in this PIA.

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).

NDR receives all data directly from Jurisdictions. Jurisdictions of Record maintain responsibility for ensuring that the information provided is accurate. Jurisdictions of Record must also correct any inaccurate information promptly. At any time, Jurisdictions of Record may request an electronic copy of all their active records on PDPS in order to review and update information. In certain circumstances, there will be time when a Jurisdiction of Record is unable to delete a pointer record. In order to assist the Jurisdiction, the NDR staff may delete a PDPS pointer record but only at the request of the Jurisdiction of Record and the correct documentation sent to NDR. For these requests, NHTSA requires that Jurisdictions verify the proposed pointer record prior to deletion.

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 protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, as updated January 22, 2015. The PDPS is a moderate risk system and was issued a three-year authority to operate on March 14, 2016. Access to the PDPS is limited to those with appropriate security credentials, an authorized purpose, and need-to-know. 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.

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 only maintains the database and is not responsible for the accuracy of the information it receives from the Jurisdiction. However, NHTSA is responsible for identifying, training and holding personnel accountable for adhering to NHTSA privacy and security policies, and regulations. NHTSA follows the Fair Information Practice Principles as best practices for the protection of information associated with PDPS. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to the protection, retention and destruction of pointer records. All NDR staff sign a non-disclosure agreement that is updated annually. NDR staff also completes mandatory annual security and privacy awareness training, as well as acknowledgement of system rules of behavior. The NHTSA Security and Privacy Officers conduct regular periodic security and privacy reviews of the system consistent with the Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Frank Subalusky
Chief
National Driver Register
frank.subalusky@dot.gov

Approval

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