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

Chou-Lin Chen
NDR_Info@dot.gov
(888) 851-0436

Reviewing Official

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

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 the Problem Driver Pointer System (PDPS) to provide a centralized repository of information on individuals whose privilege to operate a motor vehicle have been revoked, suspended, cancelled, denied, or who have been convicted of serious traffic-related offenses.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driver licensing officials search PDPS to determine if the license or privilege to drive a motor vehicle has been withdrawn.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 on March 4, 2019. NHTSA reviews and updates this document regularly to provide up-to-date information and 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 managed 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 PDPS

The records maintained in PDPS consist of problem driver identification information, and suspension or revocation status of drivers about whom a Jurisdiction has a driver record.

The PII elements that are maintained in the PDPS system include:

[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).

1. Full legal name
2. Date of birth (DOB)
3. Driver license number (DLN)
4. Individuals' aliases,
5. Social security number (SSN),
6. Gender, height, weight, sex and eye color.

Full legal name and DOB are used for performing a search on an individual on PDPS.

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 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, where an individual's driver status and licensing history are maintained.

Return of Data to Jurisdiction

Once a user is pointed to the Jurisdiction, 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 included in the result. PDPS only queries for first and last name, and DOB, but certain Jurisdictions include more data when they submit information to PDPS. That information will be returned as a result of the query.

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 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

[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

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 a Privacy Act System of Records (SORN). See DOT/NHTSA 417 – National Driver Register.[4]

NHTSA maintains a public website which includes the most up to date information on NDR and the PDPS.[5]

Additionally, NHTSA also informs the public that their PII is collected and stored through this Privacy Impact Assessment (PIA) to inform the public that their PII is stored and used by the system. The PIA identifies the information collection's purpose, use, and storage of PII. It can be found at: https://www.transportation.gov/individuals/privacy/national-driver-registry-ndr-problem-driver-pointer-system-pdps-pia

Consistent with the requirements of the Privacy Act, NHTSA published a System of Record Notice (SORN) in the Federal Register notifying the public about the NDR's classification as a system of records. DOT/NHTSA 417 - National Driver Register, NDR - 65 FR 19548 - April 11, 2000.

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.

It is the responsibility of the Jurisdiction of Record to provide notice to the individual how to access, amend or delete information about the individual 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 identification to PDPS, individuals must contact the reporting Jurisdictions of Record

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

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. 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 email to NDR_Info@dot.gov.

Under the provisions of the Privacy Act, individuals may also 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, 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 Highway Traffic Safety Administration (NHTSA)
National Driver Register, NSA-220
1200 New Jersey Avenue, S.E.,
Washington, DC 20590

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.

NHTSA's PDPS is maintained pursuant to Title 49 of U.S. Code, Chapter 303.

PDPS collects PII 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.

NHTSA collects, uses, and retains in PDPS only the data elements that are relevant and necessary for the purposes of assisting Jurisdictions of Inquiry across the United States in exchanging information about the motor vehicle driving records of individuals. This allows 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.

Under the approved National Archives and Records Administration (NARA) records schedule (N1-416-09-001), NHTSA retains all PDPS for a period of 7 years.

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 Jurisdictions. The staff at NDR does not access PDPS records unless the Jurisdiction of Records requests help to delete a pointer record, and/or a notarized Privacy Act request is mailed from the subject of the record or the individual's representative. NHTSA does not

use the information in any other manner other than allowed by Federal law and described in this PIA.

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 Secure File Transfer Protocol (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 such as the National Transportation Safety Board 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.

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 to review and update information.

PDPS performs mandatory information checks to prevent duplicated records. The full name if the individual and date of birth are mandatory data elements, and the combination of both data elements make that record unique. When a Jurisdiction submits two records with the same name and date of birth, PDPS considers them as duplicate records and the system sends them back to the Jurisdiction for correction.

In certain circumstances, there will be time when a Jurisdiction of Record is unable to delete a pointer record. To assist the Jurisdiction, the NDR staff may delete a PDPS pointer record but only at the request of the Jurisdiction 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 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 PDPS 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 PDPS system and information.

NHTSA maintains the security of PII in the PDPS system through each step in the data collection process. Security varies depending on the technology to collect the information, the format of the data and the manner in which it is transferred to the PDPS database.

Data collected and accessed through DOT laptop technology is encrypted and FIPS 140-2 compliant. Information is securely sent to the PDPS database using secure file transfer protocols to ensure the data is encrypted and protected while in transit. When a file or

document must be shipped, NDR employees or contractors use an overnight carrier such as the USPS, FedEx, or UPS. Such documents are stored in file cabinets in a secured room.

NHTSA employees and contractors with NDR access must adhere to DOT policy and procedures to ensure that the data collected, regardless of form, is protected from any misuse or unauthorized disclosure. Furthermore, all NDR users are required to take security training and sign a Rules of Behavior (ROB) document prior to obtaining access to any NDR system assets.

Further protection of PII in NDR include:

- All NHTSA employees and contractors undergo the mandatory DOT background checks prior to being granted access to the DOT network. In addition, all NDR users receive both general, and role-based security training on an annual basis.
- Use of locked cabinets and authorized document carries to ensure that hard copy files, CDROMs or USBs are appropriately secured from unauthorized access.
- NHTSA utilizes role-based security in NDR to restrict user access to specific applications.
- NHTSA enforces assigned authorizations in NDR for controlling access to the system using multi-factor authentication technology.
- The NDR system maintains an audit trail of changes made, date/time of change and the user for each database change.

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 operating administration personnel accountable for adhering to NHTSA privacy and security policies, and regulations. NHTSA follows the fair information practice principles (FIPPS) as best practices for the protection of information associated with the records in the PDPS System. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to the protection, retention, and destruction of 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 will conduct periodic security and privacy reviews of the PDPS System 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/CIOP - Privacy Risk Management - 1351.18 - Policy - 09302014.pdf.

Responsible Official

Chou-Lin Chen
System Owner
Associate Administrator, National Center for Statistics & Analysis

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

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.04.19 13:32:46 -04'00'