U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration (NHTSA)

Drug Recognition Expert Data System (DRE)

Responsible Official

Nanda Srinivasan
Associate Administrator for Research and Program Development
Email: nanda.srinivasan@dot.gov
Phone Number: 202-366-0179

Reviewing Official

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

Executive Summary

The National Highway Traffic Safety Administration's (NHTSA) mission is to save lives, prevent injuries, and reduce economic costs due to road traffic crashes, through education, research, safety standards, and enforcement. Pursuant to 23 U.S.C. Chapter 4, NHTSA is authorized to work with a wide variety of public and private partners to research and develop programs designed to increase traffic safety. One area of research is to improve ways to address impaired driving resulting from drug and alcohol use.

Aligning NHTSA's mission and to comply with 23 U.S.C. Chapter 4, NHTSA developed the Drug Recognition Experts (DRE) Data System (hereafter referred to as DRE System) to track current drug use trends and to identify emerging threats to highway safety such as spotting new drugs being used by our nation's drivers. The analyses from the DRE System serves to evaluate the effectiveness of countermeasures intended to increase highway and traffic safety, including occupant protection, and alcohol-and-drug-impaired driving technologies and future initiatives.

This Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 because the DRE System maintains Personally Identifiable Information (PII) on members of the public.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The DRE System is a NHTSA-owned and operated database that serves as a repository for data on drug-impairment evaluations of motorists suspected of driving under the influence of drugs. The DRE System's main function is to analyze drug-impaired driver's data at regional, state and national levels, to help government officials identify dangerous emerging trends in drug-impaired driving and aid local law enforcement authorities in determining appropriate countermeasures to improve highway safety.

The DRE System supports the Drug Evaluation and Classification (DEC) program in the collection and analysis of data. The DEC Program trains police officers and other public safety officials as certified drug recognition experts or drug recognition evaluators (hereafter referred to as Evaluators). Once certified, the DRE can evaluate drivers who are suspected of driving under the influence of drugs when traditional testing methods reflect the lack of presence of alcohol.

NHTSA does not have the authority to assist law enforcement officers, but under 23 U.S.C. Chapter 4, Section 403, has the authority to collect and analyze data to increase highway and traffic safety, including alcohol-and-drug-impaired driving.

How the DRE System Obtains Data

When a driver suspected of being under the influence of a substance that can impair their driving and is stopped by a law enforcement officer, a local Evaluator may perform a drug-impairment evaluation of that individual. For each evaluation performed, a law enforcement officer who serves as the Evaluator completes the collection of data items and narrative report. After the field observations are made, the Evaluator submits an electronic transcription of the collected data to the DRE System database.

If the subject of the evaluation provides a biological sample for testing, the sample is then sent to a lab for toxicology analysis. After the toxicology results are returned to the Evaluator for that specific case, the Evaluator then enters the results into the DRE System and links them to the original collected data and assessment. The system uses an algorithm to compare the Evaluator's opinion and the results of the toxicology report to gauge the accuracy of the Evaluator's initial assessment.

There are two ways in which the data is entered into the system by the Evaluator:

1. The data can be entered from any web browser and can be done during or after the field observation time frame.

2. Some states or regions have their own systems into which they enter the collected data. For these states and regions, NHTSA provides guidance on how to format their data to send to NHTSA as a JavaScript Object Notation (JSON) file. This data is sent on a regular basis (monthly, quarterly, etc.). After NHTSA receives these files, the formatting is checked for accuracy and the data is then loaded into the DRE System's database for consumption. The JSON files are sent in an encrypted format to NHTSA by the states.

Records in the DRE System

The records in the DRE System are related to the evaluation of individuals suspected of driving while drug impaired. The Evaluator does not submit the name, address, social security number (SSN) or other information that would directly identify the subject of the evaluation. Without such data, the subjects of the evaluation are deidentified and the ability to identify an individual in the DRE System's database is severely circumscribed.[2] The PII collected by the DRE system includes:

- Evaluator's Record
  - Evaluator's State, Region and Agency
  - Evaluator's Username (ID)
  - Evaluator's First and Last Name
- Subject
  - Race/Age/Gender
  - Vehicle Type

[2] To identify an individual in the DRE System would require several steps and access to multiple systems that are owned by different jurisdictions. To obtain the identity of an individual, a person would have to have access to the DRE System to obtain the local law enforcement case number. Then the individual would have to access the local law enforcement data base and search by the case number to learn the identity of the individual. To prevent such ability, access to the DRE System is limited, as discussed in the section "Access to the DRE System."

- Crash Type

The DRE system uses a standard data collection format that currently require Evaluators to complete the following data fields for each drug-impairment evaluation:

- Date/time of evaluation,
- Subject's gender,
- Subject's age,
- Subject's Breath Alcohol Content (BAC) (if obtained), and whether or not toxicology results will be available,
- Opinion of the evaluator (drug category believed to be impairing substance),
- Medical, alcohol, non-impairment rule out,
- Medical Marijuana card-holder status,
- Nature of the alleged offense (felony or misdemeanor),
- Toxicology results (drug category and specific drug),
- Law enforcement officer's name (last, first),
- Unique Case Number.

No other information is entered in the DRE System.

Access to Records in the DRE System

Access to records in the DRE System is limited to individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. Only authorized personnel can access the system and they must receive permission from the System Owner.

Access to the DRE System is based on the principle of least privilege and is granted in accordance with roles and responsibilities. The local DREs have access and limited NHTSA personnel have access. Each DRE System user can only view records that are related to their level of responsibility:

1. Evaluator: is the individual who captures the data for the DRE system and has access only to records they submitted.
2. Agency Coordinator: is the lead coordinator of the DRE program for a specific Federal, State, or local law enforcement agency that includes certified DREs. This individual can access the records of the DREs within the specific law enforcement agency.
3. State DRE Coordinator: is a law enforcement official who coordinates the DRE program for an entire state. The State DRE Coordinator has access to all the records of the Agency Coordinator within the State regions.
4. Regional Coordinator: These individuals can view records of the States under their purview.

A limited number of NHTSA employees, its contactors, also have access to all the DRE System records.

How does NHTSA use the information in the DRE System?

Information in the DRE System is used in two different ways:

1. The system can generate detailed de-identified reports to describe and depict trends in drug-impaired driving. These reports provide NHTSA, the International Association of Chief of Police (IACP), State and local law enforcement entities with information critical to understanding drug and alcohol impaired driving. It also provides authorized Federal, state, and local users with summary reports and statistical data on the number, frequency and types of drug-impaired assessments performed at national, regional, state, and agency levels. This helps identifying dangerous emerging trends in drug-impaired driving and are used to assists with the development of appropriate countermeasures.
2. The system also assists state managers in providing oversight to the DRE process. It is used to identify areas for improvement for the Evaluators during the drug-impaired evaluations such as identifying indicators of new substances which can contribute to impair driving, substance abuse, and to track the certification expiration of Evaluators.

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[3], 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[4].

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

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

personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

This PIA is intended to provide public notice of the existence of the DRE System, collection by NHTSA of the DEC evaluation data, and any associated privacy risks and mitigation controls applicable to that collection.

23 U.S.C. Chapter 4 §405. National priority safety programs authorize NHTSA to create a training on the use of alcohol and drug screening and brief intervention.

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: Privacy Impact Assessments | US Department of Transportation.

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.

The records submitted to the DRE System by Evaluators are obtained during a motor vehicle traffic stop to investigate driving while impaired. Each jurisdiction is responsible for enforcing its impaired driving laws, while providing individuals their due process rights when charged with an offense. Individuals can address the propriety of the impaired driving charge through the judicial process. Because the DRE System's records derive from State and local jurisdictions, individuals must address any issues concerning the data with the jurisdiction directly to request changes and information. If the Evaluator's data is incorrect, the jurisdiction of record must notify DRE System staff to correct the information in the database.

The DRE System contains records related to individuals who are evaluated under the drug classification and evaluation program to determine the type of drug that may have caused the impairment. The purpose of the system is to collect data on the use of drugs, impaired driving characteristics and identify trends to support the development of countermeasures that reduce impaired driving. The names of the subject of each evaluation are unnecessary for purposes of the system. Accordingly, NHTSA does not obtain the name, SSN, or other unique identifier that would permit NHTSA to identify a specific individual that is the subject of the evaluation. Individuals suspected of driving while impaired who believe they may have information recorded to DRE System should contact the law enforcement agency

for whom the Evaluator works to obtain information about him or her that may have been uploaded to the DRE System.

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.

Pursuant to 23 U.S.C. § 403[5], NHTSA is authorized to conduct research and demonstration activities, including demonstration projects and the collection and analysis of highway and motor vehicle safety data and related information needed to improve traffic safety.

Accordingly, the DRE System collects only the necessary information and provides the data to local, state, regional and national representatives to identify dangerous emerging trends in drug-impaired driving. This data helps the authorities in the development of appropriate countermeasures to improve traffic safety.

Furthermore, NHTSA may only disclose the information in a manner that does not identify individuals. Accordingly, all the DRE System reports with collected data from impaired drivers are deidentified prior to its distribution.

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 collects PII data that is relevant and necessary to analyze the data as a whole and that is necessary only for the purposes of identifying dangerous emerging trends of individuals driving under the influence of a substance that can impair his or her driving. The PII is collected by an Evaluator and provided at the time of the stop when the Evaluator suspects impaired driving, and ensures that the most accurate information is obtained, researched, and analyzed to improve traffic safety.

[5] Section 403 permits the collection of motor vehicle safety data to:
(A) all aspects of highway and traffic safety systems and conditions relating to--
(i) vehicle, highway, driver, passenger, motorcyclist, bicyclist, and pedestrian characteristics;
(B) human behavioral factors and their effect on highway and traffic safety, including--
(ii) impaired driving;
(C) an evaluation of the effectiveness of countermeasures to increase highway and traffic safety, including occupant protection and alcohol- and drug-impaired driving technologies and initiatives;
(D) the development of technologies to detect drug impaired drivers;
(F) the effect of State laws on any aspects, activities, or programs described in subparagraphs (A) through (E).

The PII that is obtained by NHTSA and retained within the DRE System pertains to drug-impaired individuals while driving and the officers who collects it. Data that is collected and used within the DRE System includes: Evaluator's information, Law Enforcement Officer's Information, Individual's race, age, gender, vehicle type (sedan, SUV or truck) and crash type, and toxicology report.

The DRE System records are scheduled pursuant to DAA-0416-2012-0005-0001, schedule approved by the National Archives and Records Administration (NARA) that permits disposal of records in the DRE System after 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.

The DRE System uses the collected information described in the Introduction and System Overview section only for the purpose of tracking current drug use trends and to identify emerging threats, and to improve the Evaluator's evaluation processes skills through training. Subject to the approval of NARA, as noted above in the Data Minimization and Retention section, NHTSA intends to keep the records in the DRE System no longer than 7 years.

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

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Manual Entry

The records in the DRE System can be collected on paper forms and subsequently transcribed into the system by individual Evaluators or can be entered directly into the system. NHTSA does not perform spot checks or otherwise quality control the data. Toxicology reports are added later after they are received by the Evaluators.

NHTSA has integrated into the system functionality (such as drop-down menus, electronic calendars and user confirmation (i.e., this is what you have entered, are you sure the data is

correct – or words substantially to that effect) designed to help eliminate the chances and decrease the probability for incorrect data capture.

The final report is manually loaded into the system and, thereafter, the individual Evaluator cannot change or amend the record content without intervention from the State Coordinator. The State Coordinator has the authority and capability to make changes to the data under his or her jurisdiction once is entered and to report they file. The have full edit access to assure quality assurance in the entire evaluation and reporting process.

State Coordinators also monitor system users, inactivate the accounts of retiring officers, and those who fail to re-certify every two years as Evaluators, or who otherwise leave the program. Former Evaluators cannot login to access evaluation records that they previously entered into the system – but the records entered by Evaluators are maintained in the system. These records are available to state, regional, and national coordinators under their purview.

Business processes that further support NHTSA's effort to ensure data quality and integrity include regular communication from NHSTA with system users and with State Coordinators to reinforce the concepts of data accuracy and integrity through web site notices, electronic newsletters, and coordinated messaging with the International Association of Chiefs of Police. NHTSA also has worked with the IACP to establish and implement business processes to ensure that the IACP issues user ID numbers to individual DREs before State Coordinators activate their accounts.

Data File Entry

Some states or regions have their own systems into which they enter their collected data. For these states and regions, NHTSA has provided guidance on how to format their data to send to NHTSA as a JSON file. Once NHTSA receives these files, they are checked for formatting and accuracy, then the data is loaded into the DRE System's database for consumption.

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.

The DRE System 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 DRE System and information. In accordance with the Federal Information Security Management Act, on an annual basis the DRE System security controls are independently evaluated, and risks addressed, as a condition for obtaining an Authorization to Operate (ATO).

NHTSA maintains the security of PII by encrypting all data communications using an HTTPS connection and use encryption technology FIPS 140-2 compliant.

Further protection of PII in the DRE System includes:

- All NHTSA employees and contractors undergo the mandatory DOT background checks prior to being granted access to the DOT network. In addition, all DRE System users receive both general, and role-based security training on an annual basis.
- NHTSA utilizes role-based security to restrict user access to specific applications.
- NHTSA enforces assigned authorizations for controlling access to the system using unique username/password combinations and roles and group membership.
- The DRE 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 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 DRE 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. The NHTSA Security and Privacy Officers will conduct periodic security and privacy reviews of the DRE 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

Nanda Srinivasan
System Owner
Associate Administrator for Research and Program Development

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: 2024.07.17 16:08:53 -04'00'