U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration

FMCSA

Study of Warning Devices for Stopped Commercial Motor Vehicles

Responsible Official

Dr. Samuel R. White
Email: Samuel.White@dot.gov
Phone Number: 202-875-1029

Reviewing Official

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

Executive Summary

The core mission of the Department of Transportation (DOT) Federal Motor Carrier Administration (FMCSA) is to reduce commercial motor vehicle (CMV) related crashes and fatalities. In carrying out its safety mission, and in accordance with 49 U.S.C. 504, 31108, 31133, 31136, 31502, and 49 CFR 1.73, FMCSA conducts research to identify and assess contributing factors associated with CMV crashes and performs analyses to identify effective countermeasures, including the use of warning devices.

As part of this effort, FMCSA established a contract with the Virginia Tech Transportation Institute (VTTI) to conduct research on the effects of warning devices deployed in association with stopped commercial motor vehicles on the behavior of passing motorists. Specifically, the planned research will leverage cutting-edge eye-tracking equipment, vehicle data sensors, and differential Global Positioning System (GPS) to characterize the drivers' detection and reaction times when on the approach to a stopped CMV in a variety of ambient conditions and in the context of different road geometries.

Due to the inherent variability in such metrics, proper research necessitates the use of large sample sizes. To encourage widespread participation, FMCSA intends to offer compensation to research participants. As a result of the applicability of tax laws to research payments, VTTI needs to collect Personally Identifiable Information (PII) from participants in accordance with issuing a W9 form. In addition, various survey and behavioral data will be collected and so it is necessary to safeguard and protect participants' privacy.

This Privacy Impact Assessment (PIA) is being conducted to address the risks associated with VTTI collecting, processing, and maintaining PII from study participants on behalf of FMCSA.

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 planned work involves an on-the-road driving experiment which will take place at VTTI within a closed-course testing facility called the Virginia Smart Roads. The goal of the research is to gather information on whether, how, and to what extent warning devices deployed in association with a stopped commercial motor vehicle affect the behavior of passing motorists in various conditions.

Participant Selection

Participants will be identified using VTTI's database of individuals who have participated in past transportation research studies at the institute and have indicated their preference to be contacted regarding future opportunities to participate in research. FMCSA intends to collect complete data from 256 participants, meaning that a somewhat larger number of participants may be recruited for the experiment, depending on loss of subjects, withdrawal, and early removal of participants from the research study.

During recruitment activities, participants will be screened for eligibility, including their driver's license status and conditions which may affect their ability to safely operate a

[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).

vehicle. This information will only be used for recruitment purposes and will not be retained or associated with data provided by participants during the research study.

Study Participation

Pre-screened participants will arrive at the facility's welcome center to report for their study appointment. To ensure the safety of both the participants and the research staff, participants will be asked to engage in a brief series of vision (acuity and color) and hearing (forced whisper) tests, as well as to provide basic demographic information and driving history. In addition, because participants will receive monetary compensation in exchange for their participation in the research, each participant will be asked to complete an IRS W9 form to ensure that VTTI complies with tax requirements.

Participants will then be fitted with eye-tracking equipment which is incorporated through wearable "glasses" and seated in the research vehicle. They will engage in an introductory/training session in which they will learn the general procedures of the study and become acclimated to the operation of the research vehicle. The research vehicle will be a standard light-duty/passenger vehicle varying only in that it includes additional equipment for data collection as well as providing a brake for operation by a member of the research staff who will be seated in the front passenger seat.

Although all participants will experience essentially the same study procedures, half will participate during daylight conditions and half will participate during nighttime (i.e., dark) conditions.

During the approximately 1.5-hour driving session, participants will periodically encounter a stopped CMV. The vehicle may be positioned either on a straight segment of road or on a curved segment of road. According to the primary experimental manipulation of interest, during each presentation of the stopped vehicle, warning devices of the type specified in 49 CFR § 571.125, often referred to as "orange road triangles", either will, or alternatively, will not, be deployed in association with the stopped vehicle according to the deployment provisions described in 49 § CFR 392.22.

Of primary interest are "detection time" and "reaction time". That is, when do participants begin to move their eyes toward their initial visual fixation upon either the warning devices or the stopped commercial motor vehicle? If warning devices enhance participants' detection of a stopped commercial motor vehicle, then it is likely that they will move their eyes toward the location of the vehicle sooner when the devices are deployed than when they are not.

Also of interest is the question of when participants begin reacting to the presence of the stopped commercial motor vehicle. Depending on a participant's behavior immediately prior to detection of the commercial motor vehicle, this response onset may manifest itself variously as a release of the accelerator pedal, the adjustment of the steering wheel angle, or

depressing the brake pedal. Vehicle sensors, combined with timing elements, will record these response onsets to provide insight into whether the warning devices affect not only detection time, but reaction time.

Of secondary interest is the characterization of participants' responses compared across the various experimental conditions. That is, does the nature of a participant's response vary reliably in response to the presence or absence of the warning devices? Vehicle sensors as well as differential GPS installed in both the research vehicle and the stopped commercial motor vehicle will assist in characterizing response variables, e.g., response amplitude. To ensure that we account for any demographically linked aspects of any observed effects, the outcomes of the research will be compared against pre-experiment survey data collected from each participant to identify any systematic effects or relationships.

Finally, upon conclusion of the study, participants will be asked to provide additional survey data regarding their experience during the driving experiment (e.g., their perception and understanding of the warning devices).

Specific data to be collected includes: (1) a demographic questionnaire (e.g., age, sex, handedness, language, education, and driving experience); (2) a hearing test to ensure participant and researcher safety during vehicle operations; (3) a visual acuity test to ensure participant and researcher safety during vehicle operations; (4) a color vision test to ensure participant and researcher safety during vehicle operations; (5) a questionnaire asking about drivers' propensity to engage in risky behavior; (6) a questionnaire to gather drivers' perceptions of warning devices encountered during the experiment; (7) instrumented vehicle data (e.g., steering input, braking input, acceleration/deceleration); (8) eye tracking data, namely measurements of the participant's point of visual fixation during driving maneuvers, as well as outward-facing camera data necessary to illustrate the point of visual fixation in space; (9) differential GPS recording the position of the instrumented vehicle on the private/closed course during the experiment; (10) Contact information (e.g., name, mailing address, email address, phone number). This information is never stored with or associated with the participant's study data.

In addition, participants will complete a W-9 form for payment/tax purposes. The completed W-9 will not be connected to the study data, and it will be stored in a locked file cabinet, within a locked office with Virginia Tech's financial managers. Physical access to VTTI information systems is restricted, limited by either key or proximity card locks. The storage of W-9 follows Virginia Tech's policy No. 1060 (https://policies.vt.edu/assets/1060.pdf). For all data collection tasks, study participants will be identified only by a researcher-assigned anonymous driver ID (e.g., Driver 001, 002, 003, etc.). All data collection instruments require use of the anonymous driver ID. The contractor keeps one separate file

that lists the driver's name along with the driver ID however, it is only accessible by the contractor's principal investigator and the chief statistician. This file is not accessible to anyone else at the contractor or FMCSA. This file is deleted one year after the project is completed, which is currently scheduled to end in September 2027. Further, this study was reviewed and has been approved by the contractor's Institute Review Board to ensure participant protection.

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.

In accordance with FMCSA's contract with VTTI to perform this research, the study will result in two datasets that are included in FMCSA's Data Repository: (1) an anonymized/de-identified public-use dataset; and (2) a limited access dataset including numbered items 1-9 as listed in the previous section in this document and partitioned according to the driver ID also described in the previous subsection. Each of these datasets is described below.

The publicly used/de-identified dataset featuring study data includes the following de-identified information from the previous section of this document:

1. Numbered items 5, 6, and 7, as described.
2. Only the eye-tracking data components of numbered item 8.
3. Numbered item 9, as described.

[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

Access to the limited access dataset will require explicit approval by FMCSA to ensure that the data is made available only to qualified researchers. A qualified researcher may request access to data from VTTI via the Data Repository.

For access to be approved, the user must show proof of Institutional Review Board (IRB) approval and sign a Data Use License (DUL) with VTTI describing their need for the limited access data. The request must also be approved by FMCSA. Identifiable data may only be viewed in the secure data enclave located at VTTI. This dataset includes video containing images of the participant driver's face while operating the research vehicle.

As this study requires the collection of data about human subjects, approval from Virginia Tech's IRB is required before data collection begins. This study was reviewed and approved by Virginia Tech's IRB (IRB #24-186). As part of the IRB process, an Informed Consent Form (ICF) was developed which details the participant's role in the study and how their data is protected. All ICFs discuss the possibility of PII being accessed by qualified researchers in a secure setting (i.e., the secure data enclave) and therefore by signing the ICF, participants agree to make their data available in this manner. The ICFs specify that a public-use dataset is to be posted online. An example of the ICF for this study has been included in Attachment A.

FMCSA informs the public that their PII is stored and used by the Data Repository via the data enclave through this PIA, published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, along with all uses of the PII stored and transmitted through the Data Repository.

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.

Before opting into participation in the study, prospective participants will be informed regarding the specific information to be collected from participants. Further information provided during the informed consent process will help to ensure the participant is capable of making an informed decision regarding the collection, use, and disclosure of their information.

Because data will be de-identified in the public dataset, there will be no way for participants to identify their data to ask for removal. Furthermore, when participants sign the ICF to participate in the study, they agree to allow their de-identified data to be posted online for future use. While all data shared on the website is de-identified, any concerns by participants may be expressed by sending an email to VTTI.

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.

This project, conducted under statutory authority granted to FMCSA via 49 U.S.C. § 31108(a)(6)(C), involves research, reporting, and development and publication of publicly-available data products in accordance with 49 U.S.C. § 31108(a)(4) resulting from motor carrier research in accordance with 49 U.S.C. § 31108(a)(3) in support of agency responsibilities under 49 U.S.C. § 31136(a), especially concerning the mission of establishing a performance baseline for assessing the effects of alternative hazard warning devices.

FMCSA and VTTI are unaware of any past or present research on the questions to be examined through the Warning Devices for Stopped Commercial Motor Vehicles study which might be used in lieu of conducting the described research.

The research and anticipated data which will result from this effort are important because they will provide much-needed insight into the safety benefits of warning devices required by regulation – including whether any such benefits exist in the first place. The intent of this work is to definitively answer the longstanding question of whether there is justification for the warning device requirements of the Federal Motor Carrier Safety Regulations. Though these devices' intended purpose is intuitive, their effects on the behavior of passing motorists, assuming they exist, are not.

Past research on the topic has critically failed to address the main aspects of safety-linked driver behavior – including the visual behavior of drivers and the nature of their control inputs when encountering a stopped commercial motor vehicle. Therefore, past work has failed to address the single most important aspect of the supposed effects of warning devices: their ability or inability to recruit drivers' visual attention toward the location of a stopped vehicle – and in so doing, hastening their response to the scenario.

The overall purpose of this collection is to answer this question and provide the agency with information on whether, how, to what extent, and in which situations warning devices deployed in association with a stopped commercial motor vehicle affect the visual and control behaviors of passing motorists.

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.

All study data is maintained or destroyed in accordance with the approved Record Disposition Schedule (RDS) Item 3, Correspondence Files, Item7A, Publications and Completed Research Products - Record Copy, Item 7B, Publications and Completed Research Products - All other copies, and Item 9, Reference Files. After the study ends, administrative data is destroyed at a predetermined date annually; this data includes participants' names, addresses, SSNs, etc. Administrative data is used to administer the study and ensure participant payment is lawfully completed. Study data, or non-identifying data collected while performing the study or calculated from data collected during the study, is processed for inclusion in FMCSA's Data Repository so that the datasets may be used for future analyses.

FMCSA determined that this collection of information is necessary for completion of the research. As stated previously, there is no existing dataset that can be substituted for the collection of data described for this research.

Participant data will be anonymized by assigning each participant a Driver at the start of data collection. That driver ID will then be linked to all data (including driving data, eye-tracking data, and questionnaire data). The only data collected during the study is the data that is needed to meet the study's objectives.

Participant data falls under the research record retention requirements found in the Department of Health and Human Services (HHS) regulations for Protection of Human Research Subjects at 45 CFR 46. The HHS protection of human subjects regulations require institutions to retain records of IRB activities and certain other records frequently held by investigators for at least three years after completion of the research (45 CFR 46.115(b)).

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 IRB process requires the researchers to provide detailed explanations of the study protocol, how data will be collected and stored, and who may have access to the data in the future. Each study approved by the IRB, including this one, also includes an ICF signed by each participant. The ICF details the types of data collected and who may have access to the data in the future. This study will only involve the collection of the data necessary to answer the research questions and that have been approved by Virginia Tech's IRB and approved via the Paperwork Reduction Act (PRA) procedures.

External researchers can request access to the limited access dataset by submitting a request on FMCSA's Data Repository website, which is managed by VTTI. For access to be approved, the requester must show proof of IRB approval and sign a DUL with VTTI describing their need for identifiable data. The request must be approved by FMCSA. The

limited access data may only be viewed in the secure data enclave located at VTTI. Researchers cannot remove PII from the secure data enclave. All personal items will be examined before the researcher can leave the secure data enclave to ensure no PII is removed.

Data Quality and Integrity

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

The Data Acquisition System (DAS) in the research vehicle will allow for the collection of high-quality behavioral data throughout the driving scenarios. For example, driving data will be collected from cameras or sensors placed on or in vehicles. Eye-tracking data will be collected from the wearable eye-tracking device worn by the participant during the study procedures. Questionnaire data will be collected directly from study participants under the assumption of accurate self-reporting. Data included in the anonymized, public-use datasets will be made available for public download. Website users are required to log in so that downloads may be tracked.

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 is protected by 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 System 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 NIST Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 2020.

FMCSA has a comprehensive information security program which contains management, operational, and technical safeguards appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII; and
- Protect against unauthorized access to and/or use of PII.

Records held by VTTI and contained in the Data Repository system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems' security and access policies. Strict controls are imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in the Data Repository system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All records in the Data Repository system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the Data Repository system is logged and monitored.

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.

Regular testing of information systems security is performed by VTTI information technology personnel. These tests include the use of assessment and scoring tools provided by the Center for Internet Security. FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training and role-based training offered by DOT/FMCSA.

This training allows individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use PII in the course of performing their duties.

FMCSA follows the Fair Information Principles as best practices for the protection of information associated with the Data Repository. In addition to these practices, policies and procedures are 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 data.

Attachment A:

Informed Consent Form (ICF)

Attachment A
Informed Consent For

Responsible Official

Dr. Samuel White
System Owner
Engineering Psychologist, FMCSA

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.10.29 09:02:20 -04'00'