U.S. Department of Transportation

Privacy Impact Assessment

Office of Inspector General

US DOT/OIG Infrastructure (GSS)

Responsible Official

Terrance King
Email: terrance.king@oig.dot.gov
Phone Number: (202)-366-7009

Reviewing Official

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

Executive Summary

The US Department of Transportation (DOT) / Office of Inspector General (OIG) Infrastructure (GSS) system is the enterprise management information system that provides local area networking (LAN) resources and access to commercial off-the-shelf (COTS) applications used by OIG staff and management for tracking and reporting capabilities in the areas of audits, investigations and mission-support services. Under the authority of the Inspector General Act of 1978, as amended, (Public Law 95-452), OIG collects, stores, and transmits sensitive information in the support of detecting waste, fraud, and abuse in departmental programs. The Act also allows US DOT OIG to collect information on any individual, subcontractors, grantees and/or incidents subject to investigations within the purview of the Act. Sensitive personally identifiable information (PII) can be collected on current and former DOT employees, DOT contractors and their employees, grantees and any other business entities and their employees. Additionally, some PII is collected through OIG public facing website (https://www.oig.dot.gov/). This Privacy Impact Assessment (PIA) documents the privacy risks and mitigations of the DOT/OIG GSS as required by the E-Government Act of 2002.

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:

[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).

- *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 Office of Inspector General (OIG) was established by law in 1978 to provide the Secretary and Congress with independent and objective reviews of the efficiency and effectiveness of the Department of Transportation (DOT) operations and programs and to detect and prevent fraud, waste, and abuse. The Inspector General Act of 1978, as amended, requires the OIG to: (1) conduct independent and objective audits and investigations; (2) promote economy, efficiency, and effectiveness; (3) prevent and detect waste, fraud, and abuse; (4) review pending legislation and regulations; and (5) keep the Secretary and Congress fully and currently informed. To fulfill these responsibilities, OIG collects, accesses, and uses significant amounts of data every day to assist with investigations and audits. With increased data collection comes increased privacy risk to DOT employees, contractors, and members of the public. To aid its mission and minimize risk, OIG utilizes the DOT/OIG GSS, which is the enterprise management information system that provides LAN resources and access to COTS applications to staff and management. These applications provide tracking and reporting capabilities in the areas of audits, investigations, and mission-support services. The DOT/OIG GSS consists of multiple subsystems performing various functions in support of the OIG mission. Data collected from these systems is stored on and maintained by the GSS, not independently therein. The OIG is committed to protecting the integrity and confidentiality of all data throughout all its component systems.

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.

The OIG builds public trust and acceptance through public notice of its information practices and the privacy impact of its programs and activities. Specifically, the OIG policy states that the OIG will:

- be transparent and provide notice to the individual regarding its collection, use, dissemination and maintenance of PII.
- maintain no system of records without first giving public notice through a System of Records Notice (SORN) published in the Federal Register.
- publish a Privacy Act Exemption Rule (Exemption Rule) for any system of records it intends to exempt from portions of the Privacy Act.
- to the extent practical, make publicly available its analysis of the privacy risks created by OIG information systems, programs or activities implemented through regulations, information collections and any implemented risk mitigation strategies. At a minimum, and to the extent permitted by law, the OIG will make publicly available approved PIAs, SORNs, Exemption Rules, and reports developed or created in response to oversight bodies including the OMB, U.S. Congress and the Government Accountability Office (GAO).
- to the extent practical, make publicly available its privacy practices, including but not limited to PIAs, SORNs and privacy reports.
- provide an online privacy policy explaining its privacy-related practices pertaining to its official external website and its other online activities.

Notice is also provided to individuals through the Privacy Act System of Records Notice (SORN) **DOT/OST 100 - Investigative Record System** - 77 FR 42797 - July 20, 2012. The SORN is available to the public on the DOT Privacy Office website

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Mapping of Appendix J Privacy Controls (Rev. 4) to Rev. 5

(https://www.transportation.gov/individuals/privacy/privacy-act-system-records-notices) and from the Federal Register (https://www.govinfo.gov/content/pkg/FR-2012-07-20/pdf/2012-17696.pdf). Investigative data compiled for law enforcement purposes may be exempt from the access provision pursuant to 5 U.S.C. 552a (j)(2), (k)(1), (k)(2), (k)(5), and (k)(7).

Additionally, the publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into the OIG GSS. This document identifies the information collection's purpose, and OIG's authority to collect, store, and use the PII and can be located at https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

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.

OIG, under the authority of Inspector General Act of 1978, as amended provide specific provisions on collecting information during investigations and audits. Data is collected and may be used to assist with investigations and audits. OIG also collects information from the general public, DOT contractors, subcontractors, and grantee via its internet web site, https://www.oig.dot.gov/. All OIG websites contain a privacy policy statement notifying visitors of data that is automatically collected.

Under the provisions of the Privacy Act, individuals may request searches of agency records to determine if any added records pertain to them. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Department of Transportation

Office of the Inspector General
Attn William Thompson
1200 New Jersey Av SE
Washington DC 20590

Department policy requires the inquiry to include the name of the individual, mailing address, phone number or email address, a description of the records sought, and if possible, the location of the records. Individuals can also email oigprivacy@oig.dot.gov for more information.

Additional information about the Department's privacy program may be found at https://www.transportation.gov/privacy-program. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

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.

OIG Infrastructure (GSS) local networking resources utilized by OIG personnel to collect, maintain, or disseminate PII during the course of their audit or investigative work is done under the authority of Inspector General Act of 1978 (as amended). OIG investigative special agents have been granted additional powers under the Homeland Security Act of 2002. This Act granted OIG investigative special agents permanent statutory law enforcement authority and allows them to make arrests, obtain and execute search warrants and carry firearms. OIG collects information throughout the investigative process, typically by interview, consent, subpoena, or search warrant. Any information collected and subsequently processed or stored by OIG case agents as part of the OIG Infrastructure system is authorized for the specific purpose of conducting such investigations. Audit work necessarily includes seeking and collecting information possibly including some PII, often pertaining to individuals, from DOT and other auditees as well as grantees, contractors, and other entities in order to report on the effectiveness of DOT programs and operations.

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.

The data that is collected in accordance with legal proceedings such as warrant, subpoena or consent pursuant to the legal authority granted to OIG investigators. Privacy information within the US DOT/OIG Infrastructure (GSS) system is retained and destroyed via policy and procedures. Records in the OIG Infrastructure are retained in accordance with the following National Archives and Records Administration (NARA) schedule DAA-0398-2013-0001

The OIG builds public trust and acceptance through public notice of its information practices and the privacy impact of its programs and activities. Specifically, the OIG policy states that the OIG will:

- be transparent and provide notice to the individual regarding its collection, use, dissemination and maintenance of PII.
- maintain no system of records without first giving public notice through a SORN published in the Federal Register.
- publish a Privacy Act Exemption Rule (Exemption Rule) for any system of records it intends to exempt from portions of the Privacy Act.

- to the extent practical, make publicly available its analysis of the privacy risks created by OIG information systems, programs or activities implemented through regulations, information collections and any implemented risk mitigation strategies. At a minimum, and to the extent permitted by law, the OIG will make publicly available approved PIAs, SORNs, Exemption Rules, and reports developed or created in response to oversight bodies including the OMB, U.S. Congress and the Government Accountability Office (GAO).
- to the extent practical, make publicly available its privacy practices, including but not limited to PIAs, SORNs and privacy reports.
- provide an online privacy policy explaining its privacy-related practices pertaining to its official external website and its other online activities.

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.

As defined in the OIG Privacy Policy, OIG programs and information systems are restricted in the collection and use of PII, or activity impacting privacy, to that which is authorized by law. As such OIG will:

- determine the legal authority that permits its collection, use, maintenance and sharing of PII, either generally or in support of a specific program or information system need.
- clearly specify usage purposes within legal authorities.
- maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

The policy also defines the internal sharing of such data as follows:

- Unless explicitly authorized or mandated by law, OIG will permit internal sharing of PII only for a purpose compatible with the original purpose of collection, specified at the time of initial collection.
- OIG will document all authorized internal sharing of PII via a Memorandum of Understanding (MOU) or other approved instrument that articulates the conditions of access and use.

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).

In accordance with OIG Privacy Policy, information shall be sufficiently accurate, complete and up to date to minimize the possibility that inappropriate information may be used to make a decision about an individual.

Additionally, OIG will:

- make reasonable efforts, prior to disseminating a record about an individual, to ensure that the record is accurate, relevant, timely.
- to the extent feasible, establish mechanisms to allow individuals to access and correct information about the individual (Part of the Privacy Act of 1974 Allow you to, on request, access and review your information held in a SOR and request amendment of the information if you disagree with it.)
- develop and implement reasonable procedures to ensure the accuracy of the data shared and the data received.
- investigate alleged errors or deficiencies in PII that has been shared in a timely manner and will correct, delete or not use the PII if found to be inaccurate.
- take timely, appropriate steps to provide written notice to the recipient of the shared data regarding any errors identified and request that the inaccurate PII be corrected or deleted.

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 USD DOT/OIG Infrastructure system is categorized with an overall risk rating of "Moderate" in accordance with Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems; and NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems. PII maintained in the system is protected in accordance with the system security plan. Access to all systems requires users to accept the "banner" acknowledging the proper use, access, and rights to the system. In addition, all users must sign OIG Infrastructure "Rules of Behavior" (ROBs) prior to access as well as annually which delineates specific handling of PII/SPII in accordance with approved OIG policy and procedures.

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.

Being a fully certified and accredited system means that US DOT/OIG system must adhere to stringent reporting and auditing to ensure the system effectively implements controls to protect the system from risks and to ensure any remaining risk is accepted by the authorizing official. US DOT/OIG Infrastructure employs controls to ensure any threats, suspicious activity, or changes to the system posture are continuously monitored. OIG security will ensure that the proper privacy controls are in place using NIST guidance and working with the DOT Privacy Office.US DOT/OIG Infrastructure has also been directly audited by the US DOT/OIG Auditors for Federal Information Security Management Act FISMA compliance. US DOT/OIG Infrastructure was also independently assessed by the Federal Aviation Administration (FAA) Electronic Services Center (ESC) each year since 2017 for FISMA control compliance. Such continuous monitoring and independent scrutiny ensures US DOT/OIG Infrastructure provides adequate protection of system data including PII and SPII.

Responsible Official

Terrance King
Chief Information Officer
Office of the Chief Information 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: 2024.09.20 10:30:23 -04'00'