



U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary

OST

DOT GrantLens

(GrantLens)

Responsible Official

Sharif Aboulnaga

Email: sharif.aboulnaga@dot.gov

Reviewing Official

Karyn Gorman

Chief Privacy Officer

Office of the Chief Information Officer

privacy@dot.gov





Executive Summary

DOT GrantLens is a secure, cloud-based enterprise web application used by the U.S. Department of Transportation (DOT) to manage the full lifecycle of discretionary federal grants across all Operating Administrations (OAs). The system provides end-to-end support for pre-award, award, post-award monitoring, performance reporting, and grant closeout, replacing fragmented legacy processes with a unified enterprise platform.

This Privacy Impact Assessment (PIA) is being conducted because the system collects and maintains Business Contact information from individuals outside of DOT to include federal personnel and representatives of State, Local, and Territorial Governments. There is also a planned implementation of a natural language Artificial Intelligence/Large Language Model (AI/LLM) search feature. The PIA addresses the privacy considerations for the use of the GrantLens system and the integrated AI/LLM search feature.

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;*

¹Office 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).



- *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 DOT is implementing the Discretionary Grants Lifecycle Management System (DGLMS) and Grants Transparency Dashboard, collectively referred to as GrantLens, as part of an enterprise modernization initiative to improve the management of discretionary grant programs across DOT OAs. GrantLens is intended to provide a unified, Department-wide capability that consolidates existing systems and processes into a single platform to enhance operational efficiency, improve data visibility, and support consistent administration of discretionary grant programs from pre-award through closeout activities.

GrantLens is a web-enabled system that provides a centralized environment for the intake, processing, management, and reporting of discretionary grant information. The system enables external applicants to submit grant applications and supporting documentation through an online portal, while authorized DOT personnel review, evaluate, and process submissions using defined workflows. These capabilities support consistent program execution across OAs and enable efficient tracking and management of grant activities within the system.

GrantLens is used by DOT personnel to manage and oversee discretionary grant programs by supporting the evaluation of applications, tracking of award decisions, and monitoring of recipient performance and financial activities. The system provides visibility into grant activity across OAs and supports program oversight and compliance functions by enabling reporting on program outcomes and performance metrics. In addition, GrantLens supports internal coordination and reporting requirements by supporting the generation and sharing of information necessary for oversight, transparency, and federal reporting activities.

GrantLens maintains information necessary to support discretionary grant program operations, including grant applications, supporting documentation, evaluation and review materials, award determinations, and programmatic, financial, and performance data. The system supports the collection and storage of information submitted through application processes. This information is used throughout the system to support program management, tracking, and reporting activities.

The Grants Transparency Dashboard component of GrantLens provides capabilities to consolidate, standardize, and present grant-related information to internal and external



stakeholders. The dashboard supports increased visibility into DOT discretionary grant programs by enabling access to aggregated and standardized data related to application activity, awards, and program performance. These capabilities enhance transparency, accountability, and compliance with federal reporting requirements, while supporting oversight by DOT leadership, external stakeholders, and the public, as appropriate.

GrantLens supports data exchange with internal DOT systems and external federal platforms to support validation, reporting, and management of grant information. These interactions enable the system to align with federal reporting and oversight requirements while reducing reliance on fragmented legacy processes and improving consistency of grant data across the Department. The system's integration capabilities support the broader goal of consolidating multiple existing systems into a unified platform and improving the efficiency and reliability of grant-related information sharing.

Applicants access the GrantLens web application and authenticate using Login.gov, eliminating the need to create a separate DOT account. Once logged in, they navigate the GrantLens portal to locate and select the appropriate funding opportunity. To begin the submission, applicants must complete the SF-424 Application for Federal Assistance, a standard government cover form that captures essential applicant details, project timelines, and funding requests to verify basic eligibility. Applicants then complete their submission by uploading this form directly through the portal along with project narratives, required and optional Notice of Funding Opportunity (NOFO) attachments, and any supplemental or follow-up documents requested by the Program Office.

For the planned AI/LLM search feature, it answers user questions by searching existing, authorized documents in real time. It will not train or update the AI model using personal or business information, so sensitive data is never permanently saved inside the model. To protect privacy, the system checks each user's access permissions before searching and only displays results that the user is allowed to see. Additionally, the system clears all search history and conversation memory as soon as the user ends their session, ensuring data is never stored or shared between users.

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) v3², sponsored by the National Institute of Standards and Technology (NIST), the Office of

² <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>



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 Organizations³.

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.

Records maintained within GrantLens are not subject to the Privacy Act of 1974 because the primary records pertain to organizations, grant projects, and federal funding allocations, rather than personal information about individuals. While business contact details (e.g., name, official email, business phone number) of applicant representatives, state/local officials, and federal personnel may be searchable or indexed within the system (including via system search and AI/LLM query features), the retrieved records remain records **about** the grant award and entity, not about the individual in their personal capacity.

Access-related logs and system activity records about individuals who access GrantLens are maintained in accordance with the Department's Privacy Act System of Records Notice (SORN), DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30758 (May 7, 2002).

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.

Submission of information for grant applications is voluntary. External applicants can manage their profile information via Login.gov and the GrantLens applicant portal.

³ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf



As stated above, only access related records are subject to the Privacy Act. Individuals wishing to know if their access records under DOT/ALL 13, Internet/Intranet Activity and Access Records, appear in GrantLens may visit <https://www.transportation.gov/resources/individuals/privacy/making-privacy-act-request> for instructions on how to request those records.

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.

DOT identifies the legal bases that authorize PII collection and specifies the purpose for which information is handled. The system supports the administration of Departmental grant programs authorized under various statutes (e.g., Title 49, U.S.C.), governed by uniform administrative requirements under 2 CFR Part 200.

GrantLens collects and maintains Business Contact information solely in an official capacity from federal personnel, state/local/territorial government officials, and grantee organization representatives. This information is limited to what is necessary to verify authorization, facilitate official communications, maintain audit trails, and administer discretionary grants throughout their lifecycle.

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.

GrantLens data are retained in accordance with DOT records management policies and applicable National Archives and Records Administration (NARA) approved records schedules. Data retention aligns with existing grant program record schedules used across DOT Operating Administrations, including General Records Schedule (GRS) 1.2 for grants management records and other applicable, program-specific disposition authorities.

All records are maintained in accordance with applicable retention periods required to support oversight, reporting, audit, and compliance activities, and remain available for historical analysis and federal audit purposes.

GrantLens consolidates data from multiple OAs. Retention practices are applied in accordance with the governing records schedules associated with the originating grant program or data source. Where records are not yet covered by an approved schedule or where updates to existing schedules are pending, such records are maintained in accordance



with DOT records management guidance until appropriate disposition authorities are finalized.

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.

GrantLens collects and maintains Business Contact PII solely to support the administration, oversight, and management of discretionary grant programs. The use of information is strictly limited to activities within the grant administration lifecycle, including application intake, evaluation, award management, recipient monitoring, and reporting. Information is not used for purposes unrelated to these authorized program functions.

System capabilities, including enhanced search or analytical functions, operate only on information already collected within GrantLens to support grant administration activities and do not introduce new uses of PII beyond the original collection purpose.

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).

Information maintained within GrantLens is obtained directly from external applicants as well as authorized DOT personnel who input, review, and manage grant-related data as part of program administration activities. Data is entered into the system through defined application interfaces and workflows, which support the consistent capture of information required for grant processing and management.

GrantLens supports standardized workflows for the collection, review, and update of grant information, which helps ensure that data is complete, consistent, and aligned with program requirements. Applicants and authorized personnel are responsible for ensuring the accuracy and completeness of the information they submit into the system. Information is maintained within the system to support evaluation, decision-making, and reporting activities.

Access to modify, update, or delete information within GrantLens is restricted to authorized DOT personnel and designated support personnel in accordance with role-based access controls and separation of duties. These controls limit the ability to alter data to personnel with defined and appropriate permissions, reducing the risk of unauthorized or unintended modification of system data.



In addition, GrantLens is designed to support auditability and traceability by capturing reviewer inputs, decision rationales, and supporting documentation as part of the grant record. These capabilities enable DOT personnel to review and validate information throughout the grant lifecycle and support oversight activities, helping to ensure the accuracy, completeness, and integrity of information maintained within the system.

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.

GrantLens is hosted in a Federal Risk and Authorization Management Program (FedRAMP) High authorized cloud environment on the Salesforce platform, which provides security controls designed to meet federal requirements for confidentiality, integrity, and availability of federal information systems.

GrantLens protects PII with administrative, technical, and physical safeguards against unauthorized access, destruction, modification, or disclosure. These safeguards are implemented in accordance with federal information security requirements established under the Federal Information Security Modernization Act (FISMA) and are aligned with Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 security and privacy controls.

GrantLens implements security controls designed to ensure that access to PII and other sensitive grant information is restricted to authorized users based on defined roles and responsibilities. Access to system interfaces and data is managed through role-based access controls (RBAC), separation of duties, and multi-factor authentication (MFA) utilizing Personal Identity Verification (PIV) credentials. These controls limit system access and data modification capabilities to personnel with appropriate permissions.

Authorized DOT personnel and designated support personnel are required to follow established policies and procedures for handling sensitive information. Personnel receive mandatory security and privacy training and are responsible for safeguarding PII in accordance with DOT policies and federal requirements.

GrantLens supports auditability and monitoring of system activity by maintaining system logs, audit trails, and records of user actions necessary to support oversight and compliance activities. These capabilities help detect and investigate potential security incidents and ensure that access to information is appropriately controlled and documented.



In the event of a security or privacy incident, GrantLens operates in accordance with DOT incident response policies and procedures, which include mechanisms for detection, response, remediation, and reporting. These processes are designed to support timely response to incidents and protection of affected information in accordance with federal requirements.

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.

Information within GrantLens is maintained and managed by authorized DOT personnel and designated support personnel in accordance with role-based access controls and separation of duties. System functionality is designed to support auditability and traceability necessary to meet oversight, reporting, and compliance requirements.

GrantLens supports auditing and monitoring of system activity using system logs, audit trails, and records of user actions and system events. Audit records are maintained to capture user activities, reviewer inputs, and decision rationales within the system, supporting oversight, audit, and compliance requirements. Auditability and traceability capabilities enable DOT personnel to assess system activity and ensure that grant-related actions are appropriately documented and can be reviewed as needed.

Access to audit logs and monitoring data is restricted to authorized systems, database, and application administrators based on their roles and responsibilities. These controls limit access to audit information to personnel with an authorized need-to-know and support the protection and integrity of monitoring data.

GrantLens operates in alignment with the Fair Information Practice Principles (FIPPs) to ensure appropriate handling and protection of PII throughout its lifecycle in accordance with federal privacy requirements. Policies and procedures governing the collection, use, retention, and protection of information are applied consistently across the system to support compliance with federal privacy and records management requirements.

DOT conducts periodic security and privacy compliance reviews of GrantLens in accordance with Office of Management and Budget (OMB) Circular A-130 requirements. These reviews, along with ongoing monitoring and risk management activities, help ensure continued compliance with applicable federal requirements and support accountability for system operations.



Responsible Official

Sharif Aboulnaga
System Owner
Supervisory IT Project Manager,

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN
MARIE
GORMAN

Digitally signed
by KARYN MARIE
GORMAN
Date: 2026.10.16
12:37:42 -0400

DOT Privacy Office - Approved - 10/16/2026



DOT Privacy Office - Approved - 10/16/2026