U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary

OST

Google Workspace

GWS

Responsible Official

Craig LaFond
craig.lafond@dot.gov

Reviewing Official

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

Executive Summary

The Department of Transportation (DOT or the Department) transitioned to the Google Workspace (GWS). Google Workspace is a FedRAMP-authorized, cloud-based suite of collaboration and productivity tools to include Gmail, Drive, Docs, Sheets, Slides, Meet, and Chat. It is used by the Department to support operational communication, document generation, information sharing, storage, and collaboration across DOT programs and components.

This Privacy Impact Assessment (PIA) is published in accordance with the E-Government Act of 2002 because GWS may contain business information and Personally Identifiable Information (PII) necessary to carry out official duties. This PIA evaluates the privacy risks, compliance requirements, and mitigation measures associated with DOT's use of GWS.

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;*

[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).

- *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

DOT uses GWS as an enterprise communications and productivity platform. The system is hosted in Google's FedRAMP High cloud environment and configured in accordance with DOT cybersecurity, privacy, and records management requirements. Access is restricted to authorized DOT personnel using DOT identity credentials and multi-factor authentication (MFA). GWS may contain business information and PII necessary to carry out official duties.

Google Workspace Employee/Contractor Access to Google Workspace

Google Workspace is only available for use by authorized DOT employees and contractors within the DOT network. Access to Google Workspace apps such as Gmail or Chat (instant messaging) is available on cloud managed Government Furnished Equipment (GFE). Regular user and admins use Single Sign-On (SSO). Super admins do not use SSO, but multifactor authentication (MFA) with National Institute of Standards (NIST) compliant cryptographic modules. GWS Service Administrators (individuals who are responsible for maintaining and configuring the GWS Tenant) coordinate with Global Administrators (GAs) (individuals with control over the Google subscription tenant) via email to assign permissions to DOT personnel for specific services. GAs adds user roles and permissions once the requestor submits the Help Desk ticket and is approved by the GWS product owner or designated individual. DOT personnel's use of GWS is subject to the DOT Rules of Behavior, which are included in the Security Awareness Training that each DOT employee and contractor must complete annually.

Google Workspace Products

DOT uses the Google Workspace Cloud to process and store data in Google production data centers. Machines supporting Google Workspace data are in Google data centers and data at rest is encrypted using full disk encryption. DOT implementation of Google Workspace services consists of Gmail, Calendar, Chat, Meet, Drive, Docs, Sheets, Slides, Forms, Contacts, Tasks, Vault, Groups for Business, Cloud Search, Keep, Sites, Gemini and NotebookLM. Google hosts the Google Workspace offering, including the underlying Google Cloud Interface (GCI) within Google data centers providing it direct control over processing and storage of the core content. "Core content" means the following subsets of Customer Data with respect to these individual components of the Services.

The DOT utilizes the following Google Workspace core and additional services to fulfill its mission. Each service is operated within the DOT's FedRAMP High security boundary:

- **Google Gmail:** Provides enterprise-grade email services for official correspondence. It processes message content, attachments, and recipient metadata, with integrated Data Loss Prevention (DLP) to monitor for unauthorized transmission of PII.
- **Google Calendar:** A scheduling service used to manage official meetings and events. It stores event titles, descriptions, participant lists, and location data to support departmental time management.
- **Gemini:** An AI-powered assistant that automates workflows and synthesizes information. Gemini within the DOT tenant operates under Enterprise terms, ensuring DOT data (prompts and outputs) is not used to train underlying models and remains inaccessible to Google personnel.
- **Google Meet:** A video and voice conferencing platform for virtual collaboration. It processes meeting details, including the meeting creator, unique access codes, and dial-in phone numbers, while enforcing encryption for all active sessions.
- **Google Chat:** A secure messaging platform for real-time communication. This includes:
  - **Direct Messages:** Individual and small-group conversations.
  - **Spaces:** Persistent group rooms used for project-based collaboration; messages within Spaces are retained indefinitely for project continuity.
- **Google Sites:** A web-creation tool used to build internal departmental portals and wikis. It stores structured web content and document links, providing a centralized hub for programmatic information sharing.
- **Google Drive:** A cloud-based storage and synchronization service. It hosts content authored by owners and collaborators, including metadata (timestamps, editor history) for all stored files within the DOT boundary.
- **Google Docs, Sheets, and Slides:** Collaborative productivity tools for word processing, data analysis, and presentations. These services process the text, data, and visual content created by DOT personnel during official document generation.
- **Google Keep**: A note-taking service for capturing quick thoughts, checklists, and voice memos. Content authored by the owner is accessible across Workspace apps to facilitate personal organization and task management.
- **Google Voice:** A cloud-based telephony service that provides assigned business phone numbers. It processes call logs, voicemail transcripts, and SMS messages, integrating with Google Vault for discovery and retention.

The organization utilizes a directory synchronization service to automate identity lifecycle management. An on-premises synchronization server performs a one-way push from the internal Lightweight Directory Access Protocol (LDAP) or primary directory to the Cloud

Service Provider (CSP). On an hourly basis, the tool audits the internal organizational schema, compiles user attributes, and securely transmits updates via HTTPS/SSL. This ensures that user accounts, groups, and contacts in the cloud environment precisely mirror the internal directory, automatically provisioning new accounts and suspending those no longer active in the primary system.

Access to Individual Email Accounts

Often requests are made that require access to individual emails within a client mailbox. These requests are for the purposes of investigations, security related alerts, containment of PII leakage incidents or other issues deemed necessary by the Office of General Counsel, Office of Human Resources or the Office of the Chief Information Officer. To access a user mailbox, a formal request must be made from Office of the Chief Privacy Officer (OCPO), Office of General Counsel (OGC), Chief Information Officer (CISO) or the Information System Security Officer (ISSM) with justification provided to the Office of the Chief Information Officer (OCIO) and Infrastructure and Operations (I&O). The I&O Branch is the only authorized mechanism for the retrieval or deletion of a specific email.

1.1 Categories of PII Collected

Google Workspace contains PII only when required for mission-related purposes. Common examples include:

- Employee and contractor contact information such as name, email, phone number
- Work-related identifiers such as office location, title, organizational affiliation
- Information submitted by members of the public in the course of DOT business including email inquiries, forms, attachments
- Business communications that include contextual PII relevant to official duties
- Document metadata including creator, editor, timestamps
- Biometric and telemetry data for Face ID and Touch ID. Telemetry data related to device authentication methods, such as Face ID and Touch ID, may be collected by devices accessing Google Workspace. Raw biometric data itself is processed locally on the device and is never shared with Google Workspace or Google.

1.2 Source of Information

- DOT employees, contractors, and candidates
- Members of the public communicating with DOT
- Other federal, state, and local partners collaborating with DOT

1.3 Purpose of Collection and Use

DOT uses Google Workspace to:

- Support communication via email and chat
- Store and collaborate on documents, spreadsheets, and presentations
- Facilitate virtual meetings
- Support workflow coordination
- Maintain and distribute work-related information

Workspace does not expand DOT's authorities or require new PII collection. It serves as a platform for existing, authorized information practices.

Generative AI Governance - Gemini & NotebookLM

- **Data Training & Privacy Isolation:** Consistent with the "Gemini for Government" terms, no Customer Data (including prompts and generated outputs) is used by Google to train or fine-tune its foundation models. DOT data remains within the DOT tenant boundary, isolated from other Google customers.
- **Human-in-the-Loop & Review:** Unlike consumer-facing AI, Enterprise Gemini does not permit Google human reviewers to see DOT data. All processing is automated and ephemeral within the DOT's FedRAMP High boundary.
- **Grounding & Retrieval Risk:** Gemini and NotebookLM utilize "Retrieval-Augmented Generation" (RAG).
- **Privacy Control:** The AI can only "see" and summarize files the specific user already has permission to access via existing Drive/Gmail permissions. The AI does not bypass existing Access Control Lists (ACLs).
- **Sensitive Data Redaction (DLP):** DOT utilizes AI-aware Data Loss Prevention (DLP) to prevent users from including high-level PII (e.g., SSNs or personal medical info) in prompts. If a prompt or an AI-generated draft contains sensitive patterns, the GWS DLP engine will block or flag the transaction in real-time.
- **NotebookLM Data Segregation:** NotebookLM is treated as a "Core Service." Sources uploaded to NotebookLM remain private to the notebook owner or specified DOT collaborators and are not indexed for general search within the DOT tenant.

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 DOT employs multiple techniques to ensure that individuals are informed of the purpose for which the DOT collects, uses, disseminates, and retains their PII within GWS.

GWE access-related records about DOT users are maintained in accordance with the Department's Privacy Act System of Records Notice (SORN), DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002, 67 FR 30758. DOT GWS is not a Privacy Act system of records that maintains Privacy Act records about members of the public; however, GWS serves as the infrastructure for the entire Department and within Google Sites, users may store official records, which could include Privacy Act records. The content stored within the system may be governed by specific programmatic SORNs of the DOT offices creating the records. It is the responsibility of the individual Google Sites site owner to ensure that transparency measures are in place to the ensure the public is aware of the policies, procedures, and technologies that directly affect individuals or their PII. The DOT Chief Privacy Office maintains a published listing of all applicable DOT, Component, and government-wide System of Record Notices (SORNs), as well as all general routine uses.

Information about the GWS program is provided to DOT employees and contractors via broadcast communications. The DOT also requires all employees and contractors to take annual security training, which includes information about data protection responsibilities. DOT's GWS implementation is not accessible to anyone outside of the DOT and, therefore, does not provide notice directly to those individuals who are not DOT users whose information it contains.

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency regarding the handling of such information.

[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

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.

Individuals whose PII is maintained in GWS may seek access, correction, or amendment to their records through the procedures established under the Privacy Act of 1974 and DOT's implementing regulations at 49 CFR § 10. Individuals may submit Privacy Act requests through DOT's established request processes.

Individuals' rights under the Privacy Act can be found here: https://www.transportation.gov/privacy-act

Google Workspace does not introduce new mechanisms for direct individual access; instead, individuals exercise their rights through DOT systems and processes, and DOT personnel retrieve records on their behalf when appropriate. When DOT collects PII directly from individuals (e.g., through forms later stored in Workspace), Privacy Act Statements are provided as required.

Information on DOT's Privacy Program can be found at https://www.transportation.gov/privacy.

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 uses Google Workspace to support authorized federal activities, including communication, collaboration, document creation, and internal operations necessary for mission execution. PII may be included in emails, documents, spreadsheets, or stored files when relevant to the official duties of DOT personnel.

DOT identifies the legal authorities for all PII collections that occur within GWS through the SORNs, Privacy Act Statements, and statutory authorities governing each program. Google Workspace itself does not expand the scope of PII collection; it serves as an enterprise collaboration platform that enables DOT staff to maintain records consistent with approved uses.

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 DOT collects and maintains only the minimum amount of information necessary for the DOT to perform its aviation safety, policy, personnel management, and other activities. Due to the range of Google Workspace products and the data present in those products, various retention schedules may be applicable.

GRS 3.1, General Technology Management Records, Item 040 {DAA-GRS-2013- 0005-0010}, Disposition: Temporary. Destroy 5 years after the project/activity/ transaction is completed or superseded. Service Level Agreements (Information technology oversight and compliance records): Information Technology (IT) Oversight and Compliance records relate to compliance with IT policies, directives, and plans. Records are typically found in offices with agency-wide or bureau-wide responsibility for managing IT operations. Includes records such as: statistical performance data; metrics; inventory of web activity; web use statistic; system availability reports.

GRS 3.1, General Technology Management Records, Item 030 {DAA-GRS-2013- 0005-0003} Disposition: Temporary Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes. Change Tickets (System development records): Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow up, and impact assessment of operational networks and systems. Includes records such as: data and detailed reports on implementation of systems, applications and modifications; application sizing, resource and demand management records; documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes; documentation of software distribution (including COTS software license management files) and release or version management.

GRS 3.2, Information Systems Security Records, Item 030 {DAA-GRS-2013-0006- 0003}, Disposition: Temporary. Destroy when business use ceases Active Directory (System access records - Systems not requiring special accountability for access): These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: user profiles; log-in files; password files; audit trail files and extracts; system usage files; cost-back files used to assess charges for system use.

GRS 5.2, Transitory and Intermediary Records, Item 010 {DAA-GRS-2022-0009-0001}, Disposition: temporary. Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule. Records that meeting the following conditions: they are required for only a short time (generally less than 180 days) and; they are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Exclusions: This item does not apply to the follow data output files, which must be scheduled on an agency-specific scheduled: files created specifically for public access purposes; summarized information from unscheduled electronic records or inaccessible permanent records; data extracts produced by a process that significantly changes the content of the file from the source records' content, effectively creating a new data file.

GRS 5.3, Continuity and Emergency Planning Records, Item 010 {DAA-GRS-2016- 0004-0001, Disposition: Temporary. Destroy when 3 years old or 3 years after superseded or obsolete, whichever is applicable. Disaster Recovery Plans and Testing (Continuity planning and related emergency planning files):Includes continuity plans or directives and supporting documentation, including but not limited to: Continuity of Operations (COOP) plans; Devolution Plans; Occupant Emergency Plans (OEP); Emergency Action Plans (EAP); Facility Emergency Action Plans (FEAPS); Records Emergency Plans (REMT); Disaster Recovery Plans (DRP); Pandemic Influenza Plans; records on continuity or emergency tests or exercises, such as: instructions to members participating in tests; staffing assignments; records of tests of communications and facilities; evaluative reports on continuity or emergency tests or exercises, such as, result reports; readiness reports; risk and vulnerability assessments site evaluations and inspections; corrective action plans; after action reports/improvement plans.

GRS 5.3, Continuity and Emergency Planning Records, Item 010 {DAA-GRS-2016- 0004-0001, Disposition: Temporary. Destroy when 3 years old or 3 years after superseded or obsolete, whichever is applicable. Disaster Recovery Plans and Testing (Continuity planning and related emergency planning files):Includes continuity plans or directives and supporting documentation, including but not limited to: Continuity of Operations (COOP) plans; Devolution Plans; Occupant Emergency Plans (OEP); Emergency Action Plans (EAP); Facility Emergency Action Plans (FEAPS); Records Emergency Plans (REMT); Disaster Recovery Plans (DRP); Pandemic Influenza Plans; records on continuity or emergency tests or exercises, such as: instructions to members participating in tests; staffing assignments; records of tests of communications and facilities; evaluative reports on continuity or emergency tests or exercises, such as, result reports; readiness reports; risk and vulnerability assessments o site evaluations and inspections; corrective action plans; after action reports/improvement plans.

GRS 5.8, Administrative Help Desk Records, Item 010 {DAA-GRS-2017-0001- 0001}, Disposition: Temporary. Destroy 3 years after resolved. Helpdesk Tickets (Technical and administrative help desk operational records): Includes: records of incoming requests (and responses) made by phone, email, web portal, etc.; trouble tickets and tracking logs; quick guides and "Frequently Asked Questions" (FAQs); evaluations and feedback about help desk services; analysis and reports generated from customer management data; customer/client feedback and satisfaction surveys, including survey instruments, data, background materials, and reports.

GRS 6.1, Email and Other Electronic Messages Managed under a Capstone Approach, Item 010 (Capstone Officials): Permanent. Transfer to the National Archives and Records Administration (NARA) after 15 years. Item 011 (All Other Employees): Temporary. Destroy 7 years after cutoff, or as authorized by specific agency-specific schedules approved by NARA. Application: This schedule applies to all Gmail content and associated metadata processed within the GWS tenant, as well as all chat/messaging functions.

The Department continues to evaluate proper retention schedules and will update this PIA accordingly.

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.

PII stored or processed in Google Workspace is used only for the purposes specified in applicable SORNs, program authorities, and internal notices. Google does not use DOT information for advertising or commercial purposes, consistent with the FedRAMP-authorized terms and federal contract requirements.
If the DOT must transmit information (such as via email) or maintain information (e.g., within a Google Sites) that comes from other Privacy Act Systems of Records, the DOT maintains and disclose that information in accordance with the applicable SORN as well as DOT Orders and Policy. Unless explicitly authorized or mandated by law, DOT permits internal sharing of PII only for a purpose compatible with the original purposes of the collection, specified at the time of initial collection.
Profile and logging PII collected by the DOT is used only as specified by the DOT's system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records*. In addition to other disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

- To provide information to any person(s) authorized to assist in approved investigations of improper access or usage of DOT computer systems.
- To an actual or potential party or his or her authorized representative for the purpose of negation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.

- To contractors, grantees, experts, consultants, detailers, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records; and
- To other government agencies where required by law.

The Department has also published additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, and July 20, 2012, 77 FR 42796, under “Prefatory Statement of General Routine Uses.”

The DOT Directory Services (DOT DS/Active Directory) exchanges authentication data with Google Workspace via Integrated Windows Authentication. GWS receives the DOT employee and contractor work contact information to ensure that Gmail emails are properly addressed and delivered to each recipient. System logs are shared with the DOT Security Operations Center for security purposes.

The DOT has authorized the internal sharing of all data associated with emails, including but not limited to all text, documents, and image files with its approved archive. GWS includes data loss prevention services designed to prevent users from sending PII and sensitive information outside of the Agency, via email.

To prevent unauthorized data exfiltration and ensure compliance with the "Least Functionality" principle (NIST SP 800-53), the DOT implements strict governance over third-party applications seeking access to the GWS environment via OAuth.

- **Restricted Access by Default:** The DOT GWS tenant is configured to "Block all third-party API access" by default. Users cannot independently authorize third-party applications to access their Gmail, Drive, or Calendar data.
- **Whitelisting Process:** Only applications that have undergone a formal security and privacy review—and, where applicable, hold a FedRAMP authorization—are added to the "Trusted" list.
- **Scope Minimization:** For authorized apps, DOT restricts access to the specific "scopes" (data fields) required for the mission. For example, an app may be granted "Read-Only" access to a specific folder rather than "Full Drive" access.
- **Continuous Monitoring:** The Office of the CISO conducts quarterly audits of all third-party integrations to revoke access for "stale" apps (those unused for 90 days) and to monitor for any changes in an app's requested permissions.

- **Agentic AI Bots:** Any AI agents or "bots" from third parties are treated as non-human identities and are subject to the same identity-first security controls and logging requirements as DOT personnel.

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).

DOT ensures that PII maintained in GWS is accurate, timely, relevant, and complete by applying standard program-level data quality procedures. GWS tools include version control, metadata tracking, and automated safeguards that reduce the risk of data corruption or loss.

Employees and contractors are responsible for ensuring data accuracy when they create, modify, or maintain records. Program offices verify the accuracy of information used in decision-making and retain validated data in appropriate systems of record.

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 DOT protects PII with 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 Security Modernization 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, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* dated September 2020.

Google Workspace is authorized for federal use under FedRAMP at the High impact level, and DOT applies additional administrative, technical, and physical safeguards to protect information against unauthorized access, disclosure, alteration, or loss. These measures include but are not limited to:

- Multi-factor authentication (MFA)
- DOT-controlled identity management
- Encryption in transit and at rest

- Access controls, logging, and security monitoring
- Google's FedRAMP-approved incident response processes
- DOT continuous monitoring and configuration oversight

Specifically, within Google Sites, the following safeguards are present:

- Google Sites are configured with Context-Aware Access policies. They are accessible only from DOT-managed devices with compliant device certificates, or via the DOT Virtual Private Network (VPN) / Trusted Internet Connection (TIC). Access attempts from unmanaged or personal devices are blocked by the Identity Provider.
- Google Sites are only accessible from Government Furnished Equipment unless approval is granted through the waiver process outlined in DOT Order 1370.121.
- Google Sites are only accessible to DOT employees and contractors with appropriate authentication.
- Google Sites are not accessible to external non-DOT users.

Additionally, within Google Sites, appropriate controls and mechanisms must be implemented to protect PII/SPII, including:

- Except for low-level PII such as name and business contact information, PII/SPII may not be stored as metadata in any list or library columns or as content on any page.
- Except for low-level PII such as name and business contact information, all documents containing PII/SPII stored in any Google Sites document library, or contained as an attachment to any list item, must be encrypted per FIPS 140-2 methodology in accordance with DOT Order 1370.121, DOT Information Security and Privacy Program & Policy.
- All PII/SPII issues reported by Data Loss Prevention (DLP) scans conducted by the Security Office must be reviewed and remediated.

Google Drive is only accessible to the assigned user unless they choose to share specific content with their DOT colleagues. It is the user's responsibility to manage the accessibility of shared content in their Google Drive by only sharing content with other DOT employees and contractors with an Active Directory account. Similarly, users of Chat are required to follow policies regarding screen sharing during meetings, including, exercising caution when sharing screens so that other users do not see sensitive or privileged information, and not allowing external parties the ability to access, open, or execute files on the host system.

DOT responds to security and privacy incidents in accordance with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII),* DOT Order 1351.29, and applicable federal guidance.

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.

DOT maintains governance, auditing, and oversight processes to ensure compliance with federal privacy laws, DOT orders, and FedRAMP requirements. These include:

- Annual Privacy Act training for all users
- Configuration and policy controls managed by the system owner and ISSO
- Regular audits of access, sharing settings, and administrative actions
- Compliance with NIST SP 800-53 privacy and security controls
- Vendor oversight and contract management
- Periodic PIA and SORN reviews

Google provides audit logs and security reports that support DOT's monitoring and risk management efforts.

Responsible Official

Craig LaFond
craig.lafond@dot.gov
System Owner
Deputy Associate CIO for Infrastructure and Operations

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN

Digitally signed by KARYN MARIE GORMAN
Date: 2026.02.11 11:21:14 -05'00'