U.S. Department of Transportation

# Office of the Secretary of Transportation OST)

# Privacy Impact Assessment
# DOT Common Operating Environment (COE)


**Responsible Official**

Jack Albright
Deputy Chief Information Officer and Associate Chief Information Officer for IT Shared Services
Office of the Chief Information Officer
jack.albright@dot.gov

**ApprovingOfficial**

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


KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.10.23 13:48:25 -04'00'

## Executive Summary

The Department of Transportation (DOT) Office of the Secretary (OST) IT Common Operating Environment (COE) is a General Support System (GSS) designed to support both small- and largescale, general- and special purpose data processing systems. It provides the essential Information Technology (IT) services and resources required to enable DOT users to perform their daily operations effectively. These services include network connectivity, domain authentication, directory services, file and print services, IT security, email, server management, and database support for both Oracle and Microsoft SQL systems.

Managed by the Office of the Chief Information Officer (OCIO), Infrastructure and Operations team, the COE delivers a comprehensive suite of shared, commodity IT services that empower DOT program offices to fulfill their mission requirements.

This Privacy Impact Assessment (PIA) is completed in accordance with 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 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 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;*

[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).

- *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 COE is the hosting environment that provides the physical and IT support (including environmental support, maintenance, monitoring, security, and administrative support) of all computers that are multi-user in nature (i.e., servers). The hosting services can be separated into two broad categories - administrative systems and application systems. The underlying technology supporting these systems is referred to as administrative servers and application servers, respectively. Administrative systems include directory, email/messaging, calendar, collaboration and other centrally hosted administrative software; and general file and print services (often referred to as General Support Systems). Application systems are generally specific to a single Operating Administration (OA) or project; however, some applications are hosted on an enterprise basis, and in these cases a single application owner represents all the users.

The Infrastructure and Operations team manages DOT IT infrastructure in accordance with shared services, including infrastructure operations, help desk, network, server, storage, desktop, Cloud, email, wireless/mobile, telephony, Internet, telecommunications, data center management, disaster recovery, and all other infrastructure/platforms as service commodity IT offerings, including assistive technologies. Operations are also managed in accordance with shared services, including Technical Architecture, Configuration Management, End User Services and Infrastructure and Service Delivery.

The COE provides the following:

- Active Directory
- Identification and Authentication Domain controller functions
- Secure Remote Access
- Database Services
- Web Hosting Services
- Messaging and Directory Services
- File/Print Services
- Service ticket management

- Server and Network Management
- Desktop and mobile device management services

The COE collects information about users, (DOT federal employees and contractors) including username, email, and file records for authorized records requests to appropriate government officials, and DOT personnel with a need-to-know to perform official duties. Specific information may include IP address; electronic mail records, including the email address of sender and receiver of the electronic mail message, subject, date, and time; user access to DOT's network and other COE enterprise systems as well as denials of access; verification and authorization of access.

## Fair Information Practice Principles (FIPPs) Analysis

*The DOT PIA template 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 PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.*

The DOT COE provides infrastructure services and minimally processes, stores, or transmits the following data elements:

- Username
- Passwords
- Images
- Email records
- Biometric identifier (e.g., fingerprints)

[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

Use of the information is contained to the support of investigative activity related to user misuse or data breach.

The Department provides general notice to the public of this records collection through its Privacy Act system of records notice (SORN), DOT ALL 13, Internet Intranet Activity and Access Records - 67 FR 30757 - May 7 2002. A comprehensive list of routine uses can be found in DOT/ALL 13 on the DOT Privacy website. There are no exemptions claimed for the system. The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency into the COE IT system. Information on the Department's privacy program may be found at www.transportation.gov/privacy.

## Individual Participation and Redress

*DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.*

The COE is a standard infrastructure which is comprised of numerous systems and networks. Systems residing on the COE may contain PII and be subject to the provisions of the Privacy Act. Systems on the COE are assessed individually and have separate Privacy documentation. Individuals can exercise their Privacy rights through the source system. For the complete list of DOT Privacy Act Systems of Records please visit: Privacy Act System of Records Notices | US Department of Transportation

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:

DOT Chief Privacy Officer
Office of Chief Information Officer
Department of Transportation
1200 New Jersey Ave., SW
Washington, DC 20590

The request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records

Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons their records must be corrected. Requests should be submitted to the attention of the OST Official responsible for the record at the address below:

DOT Chief Privacy Officer
Attn: System Manager
Office of Chief Information Officer
Department of Transportation
1200 New Jersey Ave., SW Washington,
DC 20590

The request must include the following information:

- Name of Individual
- Mailing address
- The name of system of records notice and ID: Internet/Intranet Activity and Access Records, DOT/ALL 13
- Phone number and/or email address.
- A description of the records sought, and if possible, the name of department where records are located.
- A signed attestation of identity
- The name and system of records number

Individuals with concerns about privacy and the COE may also email the DOT Privacy Officer at privacy@dot.gov or via the contact information provided in the privacy policy on the DOT's web site (www.dot.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 its collects, uses, maintains, or disseminates PII.*

COE system is used by authorized personnel to assist personnel, plan, and manage system services and perform their official duties. It is also used to monitor improper use, investigate improper activity by an employee, contractor, or other individual relating to DOT computer system use or access. In addition, The COE infrastructure includes several applications to facilitate user functions. The applications that collect PII provide specific notice and consent information. A System Use Notification message to inform users that (a) they are accessing a United States Government information system; (b) system usage may be monitored, recorded, or subject to audit; (c) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (d) the use of the system indicates consent to monitoring and recording. IT COE stores or transmits PII and non-PII and makes these data available to appropriate personnel involved in desktop and network operations. These staff members use the network to conduct

daily operations. PII related to and provides information about COE users, including username, email, and file records for authorized records requests to appropriate government officials, and DOT personnel with a need-to-know to perform official duties. Specific information may include IP address; electronic mail records, including the email address of sender and receiver of the electronic mail message, subject, date, and time; user access to DOT's network and other COE enterprise systems as well as denials of access; verification and authorization of access.

The COE IT system has the authority to collect PII in its system under 49 U.S.C. 322, General powers. These records are protected under the Privacy Act System of Records, DOT/ALL-13, Internet/Intranet Activity and Access Records.

## 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. DOT should retain PII for only if necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.*

The DOT COE provides infrastructure services and minimally processes, stores, or transmits only PII that is relevant and necessary for the specified purpose for which it was originally collected. PII use is contained to the support of investigative activity related to user misuse or data breach. The PII found in the DOT COE includes the following data elements:

- Username
- Passwords
- Images
- Email records.
- Biometric identifier (e.g., fingerprints)

The minimum and necessary PII is collected in the COE in accordance with the system of records notice DOT/ALL 13. Records are maintained and disposed of in accordance with NARA's approved record schedules below:

- 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.

- 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.

- *GRS 3.2,* Information Systems Security Records, Item 030, DAA-GRS-2013-0006-0003. Disposition: **Temporary.** Destroy when business use ceases.

- 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.

- GRS 5.8, Administrative Help Desk Records, Item 010. DAA-GRS-2017-0001-0001. Disposition: **Temporary**. Destroy 3 years after resolved.

## 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 DOT COE is a GSS that is dependent on the routers, switches, interconnections, servers, Cloud services, other IT platforms and the user workstations that are part of the DOT Wide Area Network (WAN). The DOT COE does not share data or interface with any systems not also hosted by the DOT WAN. Authorized agreements are in place for Cloud providers. Information in the system is limited to those who have a need to know in accordance with their job training. DOT does not share information from its network or IT systems in any other way.

Records in the system are covered under DOT/ALL-13, Internet/Intranet Activity and Access Records, 67, FR 30758, May 7, 2002, and may be disclosed outside of DOT as a routine. A comprehensive list of routine uses for DOT/ALL 13 can be found at in DOT/ALL 13 and DOT Blanket Routine Uses.

## 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).*

Individuals and DOT OAs are responsible for ensuring the accuracy and quality of the data submitted into the DOT COE IT system. This is done by use of Varonis. Varonis is a comprehensive data security platform that provides file integrity checks for Windows systems. It utilizes advanced data classification and security auditing capabilities to monitor file shares. The DOT uses it to automatically discover and classify sensitive data, detects suspicious activity, and provides automated remediation policies to manage access and protect against cyber threats. This allows for accelerated cross-platform security investigations and helps prevent data breaches and ensure compliance.

## Security

*DOT shall implement administrative, technical, and physical measures 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.*

Reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure are in place to protect PII. These safeguards incorporate standards and practices required for Federal information systems under the Federal Information System Management Act (FISMA), and as 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 (includes updates as of Dec. 10, 2020).

IT data files are maintained in a secure government facility and enforced with by access control measures and technologies. All IT support staff and contractors undergo background checks, are briefed on IT security requirements and associated responsibilities.

IT staff and contractors with access to COE data receive basic security training with some privacy components. These users also annually read and sign a Non-Disclosure Agreement containing privacy provisions and penalties for unauthorized disclosure of data. In addition to physical access, electronic access to PII is limited according to job function. DOT controls access privileges according to a documented roles matrix, with individuals receiving the minimum necessary access to PII and permissions. Many IT users receive read-only access to all or some of the data.

The DOT Privacy Risk Management policy requires that all PII be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards. The DOT Privacy Officer is engaged in the risk determination process and takes data types into account. The COE implements NIST 800-53 rev 5 controls to ensure the quality of data stored or transmitted by DOT Information systems and implements technology to ensure the integrity of said data in accordance with NIST 800-53 rev 5 standards. Employee access to DOT information systems is limited and must be authorized to access the data in the system.



## 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.*

The COE conducts regular periodic security and privacy compliance reviews consistent with the requirements of the OMB Circular A-130, Section 8b (3), Securing Agency Information

Systems. The COE leverages audit provisions to ensure proper usage by authorized users and monitoring for unauthorized usage. The Security Operations Center (SOC) reviews files to ensure all security and privacy protocols are adhered and followed by DOT personnel. The SOC is responsible for monitoring, detecting, and responding to potential threats across DOT's digital environments, including networks, devices, applications, and data stores. They utilize advanced tools such as Security Information and Event Management , Endpoint Detection and Response , and Extended Detection and Response technologies to ensure comprehensive visibility and threat protection. The SOC also coordinate security policies and practices, ensuring that all cybersecurity technologies work together effectively to safeguard DOT's digital assets. By maintaining a proactive defense posture against cyber threats, the SOC contributes to the overall resilience and safety of DOT's IT infrastructure.

## Responsible Official

Jack Albright
Deputy Chief Information Officer
Office of the Chief Information Officer
jack.albright@dot.gov

## Approving Official

Karyn Gorman
DOT Chief Privacy Officer
Office of the Chief Information Officer