U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary (OST)
Consolidated Automated System for Time & Labor Entry (CASTLE)

Responsible Official

Greg Gray
Information System Owner
Associate Director, Office of Financial Management, B-30
Office of Budget and Financial Management
Email: gregory.gray@dot.gov

Approving Official

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



Executive Summary

The Consolidated Automated System for Time and Labor Entry (CASTLE) is the Department of Transportation's (DOT) enterprise timekeeping and labor distribution system. CASTLE does not directly process or disburse monetary payments; instead, it serves as the primary system of record for capturing, validating, and managing the time and labor data for downstream payroll processing to DOT civilian employees. The Office of Financial Management (OFM) uses CASTLE to manage critical personnel workflows, including telework and remote work agreements, voluntary leave requests and leave banks, overtime authorizations, furlough status, offboarding, and related financial and payroll operations. Beyond core operations, CASTLE integrates two primary components: the Interface Repository (IR), which serves as a central hub for securely exchanging personnel and payroll data with external systems such as the Department of the Interior's (DOI) Federal Personnel and Payroll System (FPPS)[1], and the Commercial Off-the-Shelf Employee Master Record (COTSEMR), a read-only repository maintaining historical payroll records for audit, and research purposes.

This Privacy Impact Assessment (PIA) is being updated in accordance with the E-Government Act of 2002 to incorporate changes since the publication of the previously published PIA and because the system maintains Personally Identifiable Information (PII) on members of the public such as former employees.

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.[2]

[1] The Department of Interior, Interior Business Center (IBC) serves as the federal shared service provider for DOT payroll operations, delivering accurate and timely paychecks and related services. To manage DOT personnel and payroll transactions, DOI maintains and operates the Federal Personnel and Payroll System (FPPS).

[2] 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).

DOT Privacy Office - Approved - 1/05/2026

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk.*
- *Accountability for privacy issues.*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Department of Transportation (DOT) uses the CASTLE as its primary web-based, intranet-facing application to manage time, attendance, leave and overtime requests, telework/remote work agreements, Labor Distribution Reporting (LDR) information, Voluntary Leave Transfers Program (VLTP), Voluntary Leave Bank (VLB), furlough status, and employee offboarding for DOT Operating Administrations (OAs). It allows employees to record hours worked, request approval and code leave taken, complete situational telework agreements, report telework hours, and specific project and tasks codes for payroll purposes. CASTLE servers are hosted at the Enterprise Services Center (ESC) in Oklahoma City, OK, with a scaled-down backup hosted at an off-site disaster recovery facility in Kansas City, MO.

CASTLE operates alongside two integrated sub-components within its security authorization boundary:

- **Interface Repository (IR):** An Oracle-based central data repository within CASTLE's security boundary that serves as a secure shared data source for DOT interfaces requiring personnel and payroll information. The IR receives data from multiple sources, including DOI FPPS and other internal DOT timekeeping systems.
- **Commercial Off-the-Shelf Employee Master Record (COTSEMR):** COTSEMR contains read-only digital images of historical payroll microfiche documents from pay period 2000-21 through 2006-07 originating from DOT's legacy Consolidated Uniform Payroll System (CUPS). It is used strictly by Payroll Liaison Service (PLS) centers to research historical pay inquiries and perform audits.

DOI Privacy Office - Approved - 11/06/2026

Access to CASTLE, the IR, and COTSEMR historical files is strictly limited to authorized personnel with valid DOT network credentials and role-based access permissions.

Core Functions & Capabilities

CASTLE supports several key operational functions across participating DOT OAs:

- **Time and Attendance (T&A) / Labor Distribution Reporting (LDR):** Tracks hours worked, leave taken, telework hours, and labor cost distribution while interfacing directly with DOI FPPS for payroll processing.
- **Telework Agreement Tracking:** Electronically processes and stores telework agreements for participating OAs.
- **Remote Work Agreement Tracking:** Electronically manages remote work agreements and approval signatures.
- **Voluntary Leave Transfer Program (VLTP) & Voluntary Leave Bank (VLB):** Enables employees to request or donate accrued leave during medical hardships. CASTLE allows employees to apply to be a recipient of VLTP, employees are allowed to electronically donate leave to recipients within DOT and outside of DOT to other government employees. VLB is supported through voluntary contributions from employees. VLB allows employees to enroll, donate leave, and request approval to use shared leave from the OA's leave bank. *(VLB is only currently utilized by the Federal Aviation Administration [FAA] and Federal Highway Administration [FHWA]).*
- **CASTLE Off-Boarding (COB):** Processes administrative documentation and tracking for employees transitioning to other federal agencies, resigning, or retiring.
- **Furlough Maintenance:** This module is used to identify employees' work status during furlough. It's used for multiple purposes, one to report furlough status and justification to OMB, and to ensure employees who are funded during a furlough are paid and employees who are furloughed and excepted from the furlough are not paid.

Personally Identifiable Information (PII) Collected and Maintained

In managing time, attendance, and administrative records for current and former DOT employees, CASTLE and its sub-components collect and store the following categories of PII:

System / Component	Specific PII Elements Collected
CASTLE & IR	Full Name, Date of Birth, Social Security Number (SSN), Employee Common Identifier (ECI), Home Address, Military Time in Service, and Employee Time & Leave Records.

DOT Privacy Office - Approved: 11/06/2025

System / Component	Specific PII Elements Collected
Telework Agreements	Employee Name, First-Line Manager Name, and Telework Worksite Address.
Remote Work Agreements	Employee Name, First-Line Manager Name, and Remote Work Duty Station Address, Pay Plan, Pay Series.
Voluntary Leave Transfer Program (VLTP)	Employee & Recipient Names, Job Position Title, Series/Grade/Pay Level, Work Email, Program Coordinator Contact Details, and Recipient Treating Physician Contact Details (Name, Address, Phone, Fax, Email, upload medical information/diagnosis).
Leave Request	Employee Name, amount of leave requested, court orders, doctor's notes, etc.
Voluntary Leave Bank (VLB)	Employee Name, Home/Work Address, Email, Assigned VLB Coordinator Details, General Reason for Request, and Treating Physician Contact Details (Name, Address, Phone Number, upload medical documentation/diagnosis from the doctor).
CASTLE Off-Boarding (COB)	Employee Name, Organization, Job Title, Supervisor Name & Email, Outstanding Government Debt Status, Student Loan Repayment Program Participation, Negative Leave Balance Status, and Optional Personal Contact Email for Post-Separation Communications.
Furlough Maintenance	Employees Name, Org, Employee Common Identification, Position title, Duty Location, Appointment Type.
COTSEMR	Historical Microfiche Payroll & Master Employee Files from Legacy CUPS Records.

DOT Privacy Office - Approved - 11/06/2026

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[3], 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

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[4].

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 in the system are retrieved by personal identifier and are subject to the provisions of the Privacy Act of 1974.

Records used for fiscal operations related to payroll, attendance, leave, budget, telework, remote work, employee offboarding and cost accounting programs are maintained in accordance with the Departments published SORN, DOT/ ALL 11 Consolidated Automated System for Time and Labor Entry (CASTLE) - 89 FR 90829 - November 18, 2024 and OPM/GOVT-1 General Personnel Records. There are no exemptions claimed for the system.

Records used for personnel transactions including modification of personnel and payroll data, payroll calculation and other human resource processes that facilitate payment of salaries to DOT civilian employees are covered under DOT/ALL 19 - Federal Personnel and Payroll System (FPPS) - 73 FR 66285 - November 7, 2008.

The publication of this PIA further demonstrates DOT's commitment to providing appropriate transparency into CASTLE.

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.

Under the provision of DOT Privacy Act/ Freedom of Information Act (FOIA) procedures, individuals may request searches of CASTLE to determine if any records may have been added or pertain to them. The FOIA is a federal law that provides individuals the right to access any DOT records unless DOT reasonably foresees that the release of the information to those records would harm an interest protected by one or more of the nine exemptions (such as classified national security, business proprietary, personal privacy, investigative documents) or

[4] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

DOT Privacy Office - Approved - 11/06/2025

release is prohibited by law. Under the provisions of the Privacy Act, individuals may request searches of CASTLE to determine if any records in the system pertain to them. Individuals may mail requests in writing to:

Director of Financial Management, OST B-30
Department of Transportation
1200 New Jersey Ave, SE
Washington DC, 20590

Individuals should include in their requests the following information:

- Name and title of the system of records from which you are requesting the search.
- Name of individual
- Mailing address
- Phone number or email address; and
- Description of the records sought, and if possible, location of records.

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

Director of Financial Management, OST B-30
Department of Transportation
1200 New Jersey Ave, SE
Washington DC, 20590

For searches of FPPS payroll related records, individuals should refer to the records access procedures and contesting records procedures in the published DOT FPPS SORN.

The Privacy Act request for records covered by a system of records notices not published by the Department will be coordinated with the appropriate customer privacy official and acted accordingly.

Additional information about the Department's privacy program may be found at: https://www.transportation.gov/privacy-program/about-us. Individuals may also contact the DOT Chief Privacy Officer at: privacy@dot.gov. For questions relating to DOT's Privacy Program please go to http://www.dot.gov/privacy.

DOT Privacy Office - Approved - 11/06/2026

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.

CASTLE collects information to fulfill basic time and attendance functions, such as recording and tracking vacation taken, personal time taken, telework time, overtime, and work projects for labor distribution. Once supervisors certify timesheets within CASTLE, the validated time and labor data is transmitted via automated interface to other DOT HR systems (such as DOI's FPPS system) to send information necessary to record employee pay and HR actions appropriately. The CASTLE system collects PII only when an individual becomes an employee of DOT.

Information in CASTLE is used to monitor and manage time and attendance functions. CASTLE uses PII to identify an individual and ensure time and attendance information is accounted to the correct individual. Data in the DOI's FPPS System of Records is to control and facilitate payment of salaries to DOT civilian employees. The authority to collect PII is governed by 49 U.S.C. 322 – General Powers; 5 U.S.C. 5101 Purpose; 50 U.S.C. 3512 - Gifts, devises, and bequests; 5 U.S.C. Chapter 53 - Pay Rates and Systems; 5 U.S C., Chapter 55 - Pay Administration; 5 U.S.C. Chapter 81 - Compensation for Work Injuries; 5 U.S.C. 5551 - Lump-sum payment for accumulated and accrued leave on separation; 5 U.S.C. Chapter 61 - Hours of Work, and Executive Order 9397 – Numbering System for Federal Accounts Relating to Individual Persons.

The IR is a data warehouse within the CASTLE boundary and is the technical solution for the DOT to collect standard interface files and additional data elements needed to satisfy DOT interface applications requirements. The IR contains records for all employees in the DOT.

COTSEMR is a copy of the historical payroll Employee Master Records (EMR) microfiche documents from pay period 200021 through pay period 200607 of the legacy system, Consolidated Uniform Payroll System (CUPS). The Payroll Liaison Service centers (PLS) use the COTSEMR data to research pay issues and audits related to data that was processed by COTSEMR folders and files are provided on a read-only basis and tied to a valid DOT credentialed user account.

DOT Privacy Office – Approved – 11/06/2025

Data Minimization & Retention

DOT should collect, use, and maintain 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.

CASTLE data are retained in accordance with DOT records management policies and applicable National Archives and Records Administration (NARA) approved records schedules. Records in the system are maintained in accordance with the following NARA records retention and schedules:

General Records Schedule (GRS) 2.3, Employee Relations Records, Item 10, *Employee relations programs' administrative records,* DAA–GRS– 2018–0002–0001, Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use; Item 40,

Telework/alternate worksite program, DAA GRS–2018– 0002–0004, Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use.

GRS 2.4, *Employee Compensation and Benefits Records*, Item 10, Records used to calculate payroll, arrange paycheck deposit, and change previously issued paychecks, DAA–2018–0002–0001: Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use. Item 30, Time and attendance records, DAAGRS–2019–0004–0002, Temporary, destroy when 3 years old, but longer retention is authorized if required for business use. Item 40, Agency payroll record for each pay period, DAA–GRS–2016–00015–0004, Destroy when 56 years old.

GRS 4.2, *Information Access, and Protection Records*, Item 130, Personally identifiable information extracts, DAA–GRS–2013–0007–0012, Temporary. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate.

The penalties for the unlawful or accidental removal, defacing, alteration, or destruction of Federal records or the attempt to do so, include a fine, imprisonment, or both (18 U.S.C. 641: Public money, property or records and 18 USC 2071: Concealment, removal, or mutilation generally).

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.

CASTLE collects and maintains employee PII solely to support the administration, oversight, and management of time and attendance and administrative records for current and former DOT employees. The use of information is strictly limited to activities within the time and attendance lifecycle, including managing work hours, leave requests, overtime requests, work agreements (telework, remote work), employee offboarding, voluntary leave transfer program and voluntary leave bank, furlough maintenance. Information is not used for purposes unrelated to these authorized program functions.

CASTLE shares PII with other HR systems, such as payroll (e.g. DOI's FPPS) and other similar systems.

The Department discloses CASTLE records to external parties only in accordance with Privacy Act authorizations and the system of records notice titled, DOT/ ALL 11 Consolidated Automated System for Time and Labor Entry (CASTLE) - 89 FR 90829 - November 18, 2024:

- Disclosure of information to the U.S. Department of Interior Federal Personnel and Payroll System (DOI FPPS) for the purpose of facilitating employee wage payments. FPPS acts as the downstream personnel and payroll processing engine, utilizing CASTLE's validated hours alongside employee HR records to calculate gross-to-net pay,

DOT Privacy Office - Approved 11/06/2026

process tax withholdings and benefit deductions, disburse payroll, and provides source data to post financial entries to the general ledger.

- Disclosures may be made from this system to "consumer reporting agencies" as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Act of 1966 (31 U.S.C. 3701(a)(3)).
- Disclosure of data to external systems must be approved through an authorized data sharing agreement.
- Additional routine uses for this system can be found in the published notice along with those in related system of records notices as follows:
    - OPM/GOVT-1 –General Personnel Records, and
    - DOT/ALL 19 - Federal Personnel and Payroll System (FPPS) - 73 FR 66285 - November 7, 2008.

Data Quality and Integrity

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

The CASTLE system employs data accuracy checks in its database software to ensure data validity and accuracy. The system is reviewed to ensure, to the greatest extent possible, the information is accurate, relevant, timely, and complete via security testing and evaluation.

The CASTLE system receives PII primarily from other HR related systems, each with data quality procedures and processes. At any time, an individual can request information on his or her PII and may request some changes as appropriate.

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.

PII is protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information System Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information, and Information Systems, dated March 2006, and NIST Special Publication (SP) 800-53 as revised, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009. The Department has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of

DOT Privacy Office - Approved 11/06/2026

PII. These safeguards are designed to achieve the following objectives: ensure the security, integrity, and confidentiality of PII:

- The CASTLE system has a Continuous Monitoring Assessment (CMA) process that supports reaccreditation/reauthorization of the system. The CMA addresses the OMB Circular A-130 requirement for annual testing.
- Encryption of PII which is stored and/or transmitted is compliant with FIPS 140-2 standards.
- The CASTLE system personnel handling sensitive information are required to undergo appropriate background checks to assess their suitability to perform in public trust positions. Additionally, all staff undergoes initial security awareness training and annual refresher training, and the procedures for properly protecting the privacy of users' personal information are stressed in this training.

The CASTLE system is designed to meet all current cyber security requirements for protecting privacy information while still allowing only authorized users the full transparency needed to complete the personnel security process for applicants, employees, and contractors. The CASTLE system records are safeguarded in accordance with applicable rules and policies, including all applicable Department automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in CASTLE is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. The CASTLE system is protected from unauthorized access through appropriate administrative, physical, and technical safeguards and all system access is logged and monitored.

The system maintains an auditing function that tracks all user activities in relation to data including access and modification. Technical security controls include firewalls, intrusion detection, encryption, access control lists, and other security methods. Department personnel and contractors supporting the system are required to attend security and privacy awareness training and role-based training offered by the Department. No access is allowed to CASTLE prior to receiving the necessary clearances and security and privacy training as required by the Department. All users at the federal level are made aware of the Rules of Behavior (ROB) for IT Systems and accept them prior to being assigned a user identifier and password and prior to being allowed access to CASTLE. The CASTLE system tracks each entry in an audit file to ensure data integrity and record accuracy.

DOT Privacy Office- Approved 11/05/2026

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.

This system implements a continuous monitoring strategy that includes a configuration management process that determines the security impact of changes to the system and its environment, conducts ongoing assessments, and reports the state of system to organizational officials. An independent assessment team is used to monitor the security controls in the information system on an ongoing basis.

Responsible Official

Greg Gray
Information System Owner
Associate Director, Office of Financial Management, OST B-30
Email: gregory.gray@dot.gov

Approving Official

Karyn Gorman
Chief Privacy Officer KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.11.06 14:40:03 -05'00'
Office of the Chief Information Officer

DOT Privacy Office - Approved - 11/06/2026