U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA) Mike Monroney Aeronautical Center Franchise Fund (MMAC-FF) Enterprise Architecture and Solutions Environment (EASE)

Responsible Official

Jill Thorpe
Email: Jill.thorpe@faa.gov
Phone Number: 405-954-3209

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

Executive Summary

The Federal Aviation Administration (FAA) Enterprise Architecture and Solutions Environment (EASE) system is a federally owned and managed system that functions as a General Support System (GSS). EASE provides hosting services for multiple federal organizations by providing or facilitating general-purpose computing services from multiple computing platforms in support of administrative and program areas on a "fee-for-service basis." The system is authorized under 49 United States Code (U.S.C.) 322, 40122(g), and 4010; 40 U.S.C. 1441; and 5 U.S.C. 302.

The FAA is publishing this update to the previously published EASE Privacy Impact Assessment (PIA), July 7, 2010, pursuant to Section 208 of the E-Government Act of 2002 because EASE collects and maintains Personally Identifiable Information (PII) from members of the public, Health and Human Services (HHS) employees and contractors, and FAA employees and contractors. Also, this update addresses changes in the system operation and to adds notification that EASE has been granted the specific legal authority for the collection of the Social Security Number (SSN).

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1] Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

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

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

Introduction & System Overview

The FAA EASE system provides hosting services for federal organizations by providing or facilitating general-purpose computing services from multiple computing platforms in support of administrative and program areas on a "fee-for-service basis." With the fee-for-service arrangement, customer applications are subject to the security and privacy requirements of the "owner" organization. EASE is authorized to collect and maintain PII, including SSNs, under 49 U.S.C. 322, 40122(g), and 4010; 40 U.S.C. 1441; and 5 U.S.C. 302. SSNs are collected and used to verify the identity and "active" status of federal employees and contractors across agencies before user accounts, associated applications and/or software access are granted to EASE customer systems. SSNs are used because of the necessity to validate users (who may have the same names, or last four digits of their SSN), across agencies.

FAA's Enterprise Services Center (ESC) manages multiple systems within the franchise fund organization providing the FAA, and other federal agencies and organizations, general-purpose computing services from multiple computing platforms. ESC provides hosting services to EASE. EASE includes a separate process to manage the applications housed within EASE. The Computer Access Request System (CARS) is the application user-account provisioning tool used for account access for only those EASE customer services applications that reside on the EASE platform. It is an integral component of EASE, providing automated processing of account requests. CARS is not available to the public. CARS is a legacy government of the shelf (GOTS) application developed and maintained by the ESC.

The CARS account management software is the only component of EASE that collects PII. The collected PII is the same for internal FAA and HHS users. CARS collects name, SSN, routing symbol, region code, business mailing address, business phone number, business email address, employee supervisor's name and phone number, contractor information

including contracting company, contractor supervisor and phone number, pay status. Authorized personnel manually enter this information into CARS. Automated agency downloads from the FAA Investigation Tracking System (ITS) for FAA contractors and the DOT Interface Repository (DOT-IR) for federal employees are used to verify employee name and SSN, prior to creation of each EASE account. For initial access all users must receive approval from their managers to access the system.

Upon approval, the request is sent to the EASE administrators who verify their employment status via data exchanges with the FAA Security and Hazardous Materials Safety (ASH) Investigation Tracking System (ITS) and the DOT Interface Repository (DOT-IR). Upon verification the users receive the web address to CARS to request a user identification (ID). The authorized users enter their SSN and, if they are verified by CARS as being federal or contractor employees, they are allowed to complete the registration.

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, 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.[2]

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.

EASE is a privacy-sensitive system because it maintains collects, uses, disseminates, and retains PII from federal employees and contractors for account creation and verification. However, EASE is not a Privacy Act System of Records covered by the Privacy Act as substantive records are not retrieved by an identifier linked to an individual. Policies,

[2] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

procedures, and practices for information storage, data use, access, notification, retention, and disposal are described herein this PIA. The FAA uses access information for purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the EASE program and/or manage the system. This use is consistent with the description in the "purpose" section in SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002).

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the EASE system.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, 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.

EASE is not a Privacy Act system of records covered by the Privacy Act because substantive records are not retrieved by an identifier linked to an individual.

For an individual's PII to be included in EASE CARS, that individual must have a business need to have access to EASE and thus require a user account. The CARS Access Control Officer approves all user access to their respective systems or software electronically using CARS. The CARS Access Control Officer reviews all submitted information from the FAA and HHS employee and contractor applicants to ensure access is limited to only approved systems or software for each applicant. Providing PII to the account management software is voluntary. However, if HHS employees do not provide the requested information, the CARS Access Control Officer will deny the request for account creation. If the request for account creation is denied, the user will not gain access to any user account for any of the applications or software that resides within EASE.

Individuals are notified of the use of the information collected within CARS upon enrollment. An approved and standardized logon banner is displayed on the FAA network to all authenticated EASE users and complies with the *DOT Cybersecurity Compendium System Use Policy*. In addition, all authenticated user's initial login to the account management software, Rules of Behavior are displayed. The Rules of Behavior are displayed on the login page semi-annually thereafter. All authenticated EASE users are instructed to contact their applicable Servicing Security Organization (SSO) to challenge any PII data item that requires correction used in account verification for the electronic interface systems of DOT Information Repository (DOT-IR) CASTLE/IR and Investigations Tracking System (ITS). DOT-IR for federal employees and ITS for FAA contractor

employees. If you have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1(888) PRI-VAC1.

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.

EASE operates under authorities 49 U.S.C. 322, 40122(g), and 4010; 40 U.S.C. 1441; and 5 U.S.C. 302. The CARS account management software is the only component of EASE that collects PII. EASE maintains the following PII on HHS employees/contractors and FAA employees/contractors: Name (first, last, middle initial, suffix), SSN, Routing symbol and region code, business mailing address, business phone number, business email address, Employee supervisor name, Employee supervisor phone number, EASE User ID and password, request number, contractor company name, contract company business phone number, contractor supervisor name, contractor supervisor business phone number.

The FAA uses the HHS employees/contractors PII for access information for purposes of creating and validating login credentials, audit trails, and security monitoring. The FAA maintains FAA employees/contractors PII from those who run the EASE program and/or manage the system. This use is consistent with the description in the "purpose" section in the applicable system of records notice, DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002). The PII in the EASE system is not routinely used for any other purposes.

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 FAA collects the minimum amount of information from FAA and HHS employees/contractors to support the EASE system account creation and validation. The FAA maintains these records in accordance with following National Archives and Record Administration (NARA) approved General Retention Schedule[3] (GRS):

GRS 3.2, *Information Systems Security Records*, approved September 2014. These records are created as part of the user identification and authorization process to gain access to systems. In addition, records are used to monitor inappropriate systems access by users. Records are destroyed when business use ceases.

[3] General retention schedules are used by the FAA to determine how long to maintain an individual's records and/or when to delete the individual's records and in order to promote consistent retention practices.

The Department has also published 17 additional routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the 75 FR 82132, December 29, 2010, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019 under "Prefatory Statement of General Routine Uses."

The system also maintains SSNs. In accordance with the *FAA Project Plan to Reduce/Eliminate the Use of Social Security Numbers*, SSNs are collected and used to verify the identity and "active" status of federal employees or contractors across agencies before user accounts, associated applications and/or software access are granted to EASE customer systems. SSNs are used because of the necessity to validate users (who may have the same names, or last four digits of their SSN), across agencies. Additionally, EASE is listed in the current *FAA SSN Reduction Elimination Plan*.

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 is collected for the purpose of validating HHS employees/contractors account creation in EASE and is limited to and for authorized use only. The use of the information is limited to identifying users within the CARS process and is not used for any purposes outside of individual identification. All authorized users are HHS and FAA employees/contractors. The FAA/DOT does not share EASE access information or use the PII for any other purpose. The system does not retrieve records using a personal identifier. The FAA/DOT limits the scope of PII collected in EASE to support the purpose specified in SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records* 67 FR 30757 (May 7, 2002).

The Department has also published 15 additional routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, 77 FR 42796, July 20, 2012, and 84 FR 55222, October 15, 2019 under "Prefatory Statement of General Routine Uses."

Finally, the FAA periodically reviews the collection, use, and disclosure of PII through its periodic review of this PIA and a Privacy Threshold Analysis (PTA).

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).

EASE collects, uses, and retains data that is relevant and necessary for the purpose for which it was collected. PII is entered directly into the system by HHS and FAA employees/contractors. Because they are the one providing their information and enter and verify that all PII entered is correct, it is assumed to be accurate. Additionally, EASE programmatic checks help verify the PII entered by authorized personnel for consistency. Examples of a programmatic check include:

- Data validation rules (i.e., a zip code has five numeric characters)
- Moving the cursor to the first empty space for required fields
- Identity verification using the separate one-way electronic interfaces, which are received weekdays from DOT-IR and ITS to prevent records with duplicate names and SSNs from being stored in CARS.

If the user cannot be verified against the daily files, the request is electronically cancelled, and an error message displayed to the submitter. If an SSN is entered that cannot be authenticated on either the DOT-IR (DOT) or ITS (FAA), the EASE account request is rejected.

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.

EASE takes appropriate security measures to safeguard PII and other sensitive data. The FAA 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 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 the National Institute of Standards and Technology (NIST) Special Publication *800-53, Revision* 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020 (includes updates as of December 10, 2020).

The FAA matches PII daily from DOT-IR and ITS against CARS, and associated logon-IDs and application access are deleted (Monday-Friday) for employees who are separated. Data in CARS is used by Access Control Officers to review account access and re-certify federal employee access annually, and contractor access semi-annually for their designated systems. Access that is not re-certified within 90 days by the access control officers for the designated system and/or software is automatically removed. DOT-IR and ITS are not hosted in the

EASE platform. The required interconnection agreements also identify the types of permissible and impermissible flows of information and data elements transmitted in the daily files received from ITS and DOT-IR. ITS and DOT-IR provide daily interfaces only (one-way) to EASE. These safeguards include an annual independent risk assessment of the EASE system to test security processes, procedures, and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to know are authorized to access the records in EASE. All data in-transit is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessment to test and validate security process, procedures, and posture of the system. Based on the security testing and evaluation in accordance with the FISMA, the FAA issues EASE an on-going authorization to operate.

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 implements 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. FAA Order 1370.121B*, "FAA Information Security and Privacy Program & Policy,"* implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with EASE are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of EASE as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Jill Thorpe
System Owner
Acting Manager Systems Operations & Managed Services Enterprise Services Center

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2025.05.01 14:51:27 -04'00'