U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration (FAA)

Office of Finance and Management (AFN)

Electronic Federal Aviation Accelerated and Simplified Tasks (eFAST) Tracking System (ETS)

Responsible Official

Alan Behr
Email: alan.behr@faa.gov
Phone Number: 301-395-1546

Reviewing Official

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

Executive Summary

The Electronic Federal Aviation Administration Accelerated and Simplified Tasks (eFAST) Tracking System (ETS) is owned and operated by the Federal Aviation Administration's (FAA) Office of Finance and Management (AFN). The eFAST is the FAA's preferred contracting vehicle for small business contracts. The AFN is responsible for streamlining agency functions and ensuring the delivery of services. The eFAST system, herein after referred to as ETS, simplifies procurement for all stakeholders by using a web-based acquisition tool and automated workflows. ETS aligns with 40 United States Code section 1441, which outlines the responsibilities regarding efficiency, security, and privacy of Federal computer systems. The ETS system supports the entire acquisition lifecycle and contract management, which includes:

- Proposal submittal
- Proposal evaluation
- Award decision and notification
- Approval of resumes, ODC, travel requests, and overtime requests
- Past performance
- Invoice review and tracking
- Fee Management.

The FAA is publishing this Privacy Impact Assessment (PIA) for ETS in accordance with Section 208 of the E-Government Act of 2002. The system processes Personally Identifiable Information (PII) from members of the public, specifically from resumes of potential hire candidates who may become authorized vendors. The PII includes name, citizenship, personal email address, education, employment information, and job titles to assess job experience for labor categories.

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;*
- *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 AFN operates the eFAST ETS, which is the FAA's primary tool for managing small-business contracts. ETS streamlines the contracting process and provides the ETS program office with a centralized view of contract status and funding to support informed decision-making. ETS operates under the authority of 49 U.S.C. § 106, 49 U.S.C. § 40110, and 40 United States Code section 1441, which outlines the responsibilities regarding efficiency, security, and privacy of Federal computer systems.

ETS streamlines procurement through a web-based interface with automated workflows. ETS is accessible to authorized vendors, FAA employees, and contractors. The system enables the eFAST office (FAA employees and contractors) to solicit, evaluate, and manage vendors and contracts. FAA employees can upload and review proposals, make award decisions, approve resumes and travel requests, evaluate past performance, review invoices, track fees and payments, comment on records, and assign work using workflows. FAA eFAST vendors, as authorized vendors, can review Screening Information Requests (SIRs), submit proposals, and provide cost and pricing information to the eFAST office for consideration in future orders. Authorized vendors may also provide additional data, such as business size and past performance.

ETS receives contract-related data from SAM.gov, a centralized platform managed by the U.S. General Services Administration (GSA) and is finalizing the memorandum of agreement (MOU) with SAM.gov. SAM.gov provides non-PII read-only data, including company name, company address, business types, and functional areas. ETS receives

[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).

procurement information from the Enterprise Data Platform (EDP), formerly the Enterprise Information Management platform (EIM) which includes data from PRISM, an internal FAA system that processes and tracks procurement documents such as non-PII related purchase requests (PR), procurement contracts (PC), and purchase orders (POs) for FAA products and services. ETS via EDP receives data from DELPHI, an eInvoicing system designed to automate invoice and payment processes. This data is read-only, does not include PII, and consists of contract-related information such as contract number, contract value, period of performance, amount invoiced, last invoice date, contract modification number, and type of contract modification.

ETS access is role-based on organizational divisions and access is deliberately limited to prevent unnecessary viewing across branches or job functions.

Typically, FAA employees and contractors log in to ETS using their Personal Identification Verification (PIV) cards for authentication via MyAccess. The PII collected is email address, first name, and last name, and is used strictly for authentication purposes.

Vendors can become authorized users by requesting an account through Login.gov. To create an account, login.gov uses an email address and name. Once authorized, vendors can access eFAST to review Screening Information Requests (SIRs).

Business Process and System Process

When a Screening Information Request (SIR) is posted in the ETS Workspace, FAA employees review and process cost and pricing information from authorized vendors. SIRs use PII, such as names, contact details (e.g., work email, work phone), work history, potential hire resumes, and past performance of vendor personnel, and job title for FAA personnel. Resume information may be stored when submitted for task orders. ETS does not collect social security numbers, financial account numbers, or health information. The collected information is used to verify qualifications, review proposals, approve travel or other costs, contact relevant personnel, and maintain accurate contract records.

FAA ETS team members track vendor evaluations, add comments to records, and use workflows to assign tasks within the eFAST office. If a team member determines the vendor to be qualified, they award a Memorandum of Agreement (MOA) through the ETS system. When a new work becomes available under ETS, it is awarded to qualified MOA holders through Task Orders in the system.

When work becomes available for an ETS MOA holder by Task Order, ETS vendors submit resumes of potential hire candidates/MoTP in the ETS system for the FAA eFAST office to review and match labor categories. The resumes may include name, citizenship, employment information, email addresses, education information, and positions or titles. To review a candidate's information relative to a Task Order labor category, the data is retrieved from ETS by either Labor Category code, Task code, or company name, not by individual name or unique identifier.

In addition, ETS vendors submit requests for travel and other direct costs using an electronic form in the ETS system. The form includes name, travel information and order of contract (ODC), and overtime requests. The FAA ETS office reviews and approves these requests during the period of performance.

All documents attached to ETS are stored in the ServiceNow cloud environment. The system restricts access so users can view only records related to their projects, contracts, or operational responsibilities. Only authorized FAA personnel can access this information, and it is not shared outside the agency unless required by law.

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 552a(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 ETS tracking tool is a privacy-sensitive system because it maintains, uses, disseminates, and retains PII from members of the public (e.g., potential hire candidates) for ETS funding contracts, including new and existing authorized vendors. ETS does not collect information directly from members of the public; instead, it receives resumes that include name, citizenship, employment information, email addresses, education, and job titles to assess experience for Task Order labor categories.

The FAA retrieves records related to candidate experience (resumes) for Task Order labor categories by labor category code or company name, not by individual name or unique identifier. As a result, these records are not covered under the Privacy Act and do not require a System of Records Notice (SORN).

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

Records used for login credentials, audit trails, and security monitoring for FAA employees, authorized users, and contractors who are part of the eFAST program and/or manage the system are subject to the Privacy Act. The use is consistent with the description in the "purpose" section in the applicable system of records notice SORN, DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002).

For account management, individuals enter their own information into ETS. Once an individual's request for a new ETS website account is approved, the user can correct their name, or email address, by contacting the ETS Customer Care at 1-877-209-0513, option 1 or by the Acquisition team at natl-efast-admin@faa.gov. For resume updates or changes, the individual would contact their company or authorized vendor, which would submit the change to the ETS help desk or the Acquisition team.

In line with the above SORN, DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002), the FAA provides a Privacy Act Statement (PAS) when users access the system, which details the purpose and authority to collect PII as well as the routine uses.

Publishing this PIA demonstrates the FAA's commitment to transparency regarding the ETS system.

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 with reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

As noted above, ETS is not subject to the Privacy Act because the records are not about individuals and are not routinely retrieved by PII. ETS does not collect information directly from individuals; it receives resumes of potential hire candidates that provide experience relevant to the task order Labor categories. Data is retrieved by Labor Category code, Task code, or company name, not by an individual's name or unique identifier.

If changes to an individual record are required in ETS, once an individual's request for a new ETS website account is approved, the user can correct their information such as name, or email address, by contacting the ETS Customer Care at 1-877-209-0513, option 1 or by the Acquisition team at natl-efast-admin@faa.gov. For resume updates or changes, the individual would contact their company or authorized vendor to submit the change to the ETS help desk or the Acquisition team.

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.

Congress has authorized the FAA Administrator to enter into contracts under several authorities, including 49 U.S.C. § 106, 49 U.S.C. § 40110. The Administrator may develop systems and /or tools to support the business need for a contracting vehicle to manage small business contracts. ETS addresses the unique demands of the FAA's workforce and is governed by Title 40 United States Code section 1441, which outlines the responsibilities regarding efficiency, security, and privacy of Federal computer systems.

ETS collects name and email address PII for FAA employees, contractors, and authorized vendors to manage the ETS software and program, as well as for authentication and access.

The FAA uses this access information to create and validate login credentials, maintain audit trails, and monitor security for FAA employees, contractors, and authorized vendors who are part of the ETS 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).

ETS collects the following PII on members of the public (authorized vendor and potential hires) through resumes during the pre-award screening process to ensure only qualified small business entities participate in FAA contracts. Resumes are used to confirm that individuals meet required qualifications, experience, and labor category standards.

- name
- citizenship (U.S. Citizen or resident alien)
- employment information (experience relative to the task order labor categories)
- home/cell phone
- work email address
- education information
- position/title.

The PII in the ETS system is not routinely used for any other purposes.

ETS is not a Privacy Act system of records for substantive records supporting contracting activities, such as reviewing proposals, confirming qualifications, approving travel and cost requests, and selecting task orders.

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 retains PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The FAA minimizes its data maintenance, use, and retention in ETS to only that information relevant and necessary to meet its authorized business purpose: supporting contracting activities such as reviewing proposals, confirming qualifications, approving travel and cost requests, and selecting task orders.

The FAA retains ETS records according to the disposition schedule, DAA-GRS-2013-0003-0001, approved April 2020, which maintains that financial transaction records are destroyed six years after final payment or cancellation.

Records supporting a compilation of agency financial statements and related audit, and all records of all other reports are retained by disposition schedule, DAA-GRS-2013-0003-0011, approved April 2020, are destroyed two years after completion of audit or closure of financial statement/accounting treatment/issue, but longer retention is authorized if required for business use.

Vendor and bidder records that include documentation of approved, suspended, and debarred vendors or bidders are retained in accordance with the disposition schedule, DAA-GRS-2016-0001-0005, approved April 2020. Records are destroyed three years after removal from approved status but longer is authorized if required for business use.

Records schedule DAA-GRS-2017-0011-0002 for Job Vacancy files of applications, resumes, supplemental forms, and other attachments, include records of standing register competitive files for multiple positions filled over a period of time, are destroyed 2 years after the termination of the register.

System access records for systems not requiring special accountability for access are governed by the National Archives and Records Administration (NARA), retained by General Records Schedule (GRS) 3.2, approved January 2023 disposition schedule, DAA-GRS-2013-0006-0003, and are destroyed when business use ceases.

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 PII in ETS is collected from authorized vendors, FAA employees and contractors to support contracting activities (e.g., proposal submission and review, resume approvals, and invoice tracking). The PII in ETS is accessible solely to FAA employees and contractors, and authorized vendors who have an official, role-based need for the data, and access is deliberately limited to prevent unnecessary viewing across branches or job functions. Access controls enforce strict separation of duties. Individuals in one branch cannot view the contract files, personnel data, or supporting documentation belonging to another branch unless their specific role authorizes it. Users cannot see data beyond the scope of their assigned duties.

Role-based permissions also prevent overexposure of information across teams, offices, and contract portfolios. The system automatically restricts access so that users view only the records associated with their projects, contracts, or operational responsibilities. The FAA does not use the PII for any other purpose.

Access and authentication records within ETS are handled in accordance with 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. These routine uses are published on the DOT General Routine Uses SORNs page.

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).

ETS collects, uses, and retains data relevant and necessary for its intended purpose. Members of the public, authorized vendors, FAA employees, and contractors with PII in the system are responsible for ensuring the accuracy of their information. ETS validates PII collected and maintained for system access through PIV. Members of the public/authorized users use login.gov which provides MyAccess an authentication token to validate the external user has authenticated with Login.gov. ETS uses PII to compare and validate information collected from user registration to ensure the correct system use is being processed. For resume updates or changes, the individual would contact their company or authorized vendor, which would submit the change to the ETS help desk or the Acquisition team. Contracting staff routinely review access information during contracting actions and update it as needed to support contract decisions.

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 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 Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of ETS 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 ETS. All data in-transit is encrypted and access to electronic records is controlled by PIV and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessment to test and validate security processes, procedures and posture of the system. Based on security testing and evaluation in accordance with the FISMA, the FAA issues ETS an on-going authorization to operate (ATO).

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.

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.

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.

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 ETS 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 ETS as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Alan Behr
System Owner
Information System Owner, Office of Finance and Management (AFN)

Approval and Signature

Karyn Gorman
Chief Privacy Officer
KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.08.25 16:02:59 -04'00'
Office of the Chief Information Officer