U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Information & Technology Services (AIT)

MyAccess

Responsible Official

Jeff Adam
9-NATL-MyAccess@faa.gov

Reviewing Official

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

[Publication Date]

Executive Summary

MyAccess collects personally identifiable information (PII) in order to perform identity management for Federal Aviation Administration (FAA) internal credentialed users such as employees and contractors and certain external non-credentialed users such as United States citizens and foreign nationals who need access to FAA Internet Technology (IT) systems that are integrated with MyAccess. MyAccess operates under statutory authority including 49 U.S.C. 44701(a)(5), 44702(a)(2), and 44703(b)(B).

The FAA adheres to the guidance set forth in Executive Order M-26-18, *Scaling Use of Login.gov to Deliver a Universal Sign-on for Public Services*, issued August 31, 2026. As a result of implementing this Order and the integration of many FAA systems with Login.gov, the MyAccess PIA is being updated to reflect changes in functionality and the collection of PII that have occurred as a result.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

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

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*

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

- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

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

Introduction & System Overview

MyAccess is an application that identifies, validates, and authenticates authorized users to access various applications located on DOT's or FAA's enterprise networks. Specifically, the FAA uses MyAccess to ensure a streamlined approach toward common business practices. This allows users of web-based applications to seamlessly connect, interact, and respond electronically to customers, stakeholders, colleagues, and resources more reliably and securely. MyAccess functionality reduces the need for passwords that would be required for accessing multiple enterprise applications on the FAA enterprise networks.

The Department has a significant business need to allow individuals external to the Department to access applications supported by MyAccess. These individuals have not previously had their identity verified by the Department, so additional processes and information collections are necessary to ensure that individuals are who they claim to be. Given the sensitive nature of the systems accessible via MyAccess, the FAA has determined that a high degree of confidence is necessary for the validity of the identity asserted by users. To achieve this level of confidence, associated with Level of Assurance (LOA) 2 as described in the Office of Management and Budget (OMB) Memorandum 04-04, "E Authentication Guidance for Federal Agencies," and Memorandum 26-18, "Scaling Use of Login.gov to Deliver a Universal Sign-on for Public Services" the FAA has partnered with Login.gov for external user authentication and domestic identity proofing. The FAA has also contracted with a third-party identity proofing services provider (IdSP) for foreign national identity verification. The IdSP is consistent with the National Institute of Standards and Technology (NIST) technical guidelines for federal agencies implementing remote electronic authentication of individuals interacting with government information systems (IT) over networks, issued in Special Publication 800-63-3, "Electronic Authentication Guideline."

Users and Authentication:

Internal Credentialed User

Internal users are credentialed DOT/FAA employees and contractors. MyAccess Workforce authenticates all DOT/FAA employees and contractors to applications that are integrated with MyAccess via Secure Assertion Markup Language (SAML) or OpenID Connect

(OIDC). MyAccess replicates DOT/FAA users from their respective Active Directory sources of truth. Users that are active in DOT and FAA Active Directory are active in MyAccess Workforce. Users that are disabled in DOT/FAA Active Directory are disabled in MyAccess Workforce.

MyAccess Workforce provides FAA/DOT PIV authentication and where policy allows, email authentication with password and phishing resistant multifactor authentication.

When using the PIV card, the DOT employee or contractor inserts their PIV card into the card reader and selects *OK* to proceed. They will then be presented and must select a certificate that includes their name, the government entity that issued the certificate, and the certificate validation dates. Once the certificate is selected, the DOT employee or contractor enters their 6-to-8-digit PIN. If the login PIN entered matches the PIN registered with a user's PIV card, then the user is looked up within MyAccess to determine if the account is active. If the account is active, then the user is authenticated.

When using email authentication, a DOT employee or contractor must enter their email address, password, and select/enroll in a phishing resistant multifactor authenticator such as Okta Verify, hardware token, Windows Hello or Apple FaceID. MyAccess Workforce locks an account for 15 minutes when 5 unsuccessful authentication attempts occur with email, password, and multifactor authentication. DOT/FAA users may perform a password reset selecting the "Forgot Password" link. DOT/FAA users may also enroll in more than one phishing resistant multifactor authenticator.

External Credentialed User

External credentialed users are employees or contractors of federal agencies/departments outside of the DOT. In compliance with OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, MyAccess has established a partnership with Login.gov. This partnership is established within the MyAccess CIAM service as an external Identity Provider (IdP). When an external credentialed user needs to authenticate to an external facing FAA resource, external users are presented with an option to login as a Customer, DOT/FAA Employee or Contractor, Other Federal Employee or Contractor, or International Customer. Other Federal Employee or Contractor option redirects to Login.gov where an external credentialed user may use their existing Login.gov account or create an Login.gov account and bind their Agency/Department credentials as an authentication method. On successful identity verification and authentication with Login.gov, the user is redirected back to MyAccess where a CIAM token is established and then redirected to the application as an authenticated MyAccess CIAM user.

External Non-Credentialed User

External non-credentialed users are members of the public, U.S. citizens, or foreign national, who are not federal government employees. Non-credentialed external users can establish an

identity assurance level 1 (IAL1) or an identity assurance level 2 (IAL2) account. IAL1 accounts allow self-assertion and are typically authorized to external-facing applications that have a low security threshold. IAL2 accounts require evidence that supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 accounts are typically authorized to external facing applications that have security thresholds that require verification that the end user is who they claim to be. IAL1 users may only authenticate to IAL1 applications protected by MyAccess CIAM. IAL2 users can authenticate to IAL1 or IAL2 applications protected by MyAccess CIAM. The application is responsible for authorization.

External U.S. Citizens may create a Login.gov account by visiting Create an account | Login.gov or by navigating to any FAA website integrated with MyAccess CIAM. Account creation via Login.gov is separate from identity verification. Identity verification is determined by MyAccess CIAM and the application the external user is trying to access. MyAccess will instruct Login.gov to verify the identity of the external user when required. External users that have previously verified identity and established an account directly with MyAccess CIAM will be required to verify identity again and migrate their account to Login.gov. Instructions for migration are provided at the MyAccess CIAM help application, https://help.myaccess.faa.gov/. User migration is performed via the migration application at https://migrate.myaccess.faa.gov. MyAccess stores the first name, last name, email address, Login.gov Unique Identifier, identity verification timestamp, and identity assurance level of external U.S. citizens. This information is obtained from Login.gov.

Foreign Nationals and ID Data Web (IDDW):

Foreign Nationals must create an account with Login.gov. When account creation is complete then as determined by an application, they may be required to verify identity. Identity verification is performed by ID Data Web, which is a software as a service (SaaS) that MyAccess uses via an Application Programming Interface (API). On successful verification, ID Data Web notifies MyAccess CIAM of the success and the Foreign National account is labeled as IAL2.

IDDW uses a compilation of databases from more than 1,000 data sources that contain both public and proprietary information to identify, verify, and authenticate Foreign Nationals information. The process for enabling identity matching of the registrant's information includes. Prior to access to an application integrated with MyAccess that requires identity verification, Foreign Nationals will be redirected to ID Data Web's application where the PII data is entered via a secure sockets layer. Once PII is received, ID Data Web performs an automated identity validation – a process that takes place on ID Data Web servers to determine if a match is located. ID Data Web notifies MyAccess with a success or failure message for ID verification. However, neither the results nor the PII matched are saved in MyAccess or ID Data Web. All ID Data Web provides back is success or failure and a

country code – no PII is provided back. MyAccess then labels the Foreign National as IAL2 for future authentication.

ID Data Web has established business agreements with several major financial services companies and banks that enable them to attempt to locate a match of the external user's phone number utility account, full name, DOB, and address. The financial institution crosschecks its financial records against information provided by the external user to determine a match and accuracy of the information provided.

ID Data Web has established business agreements with cellular telecommunication companies that enable them to attempt to locate a match of the external user's mobile cell phone number to that of the applicable individual wireless account within a cellular telecommunication company.

MyAccess only produces administrative reports accessible to MyAccess administrators. MyAccess can produce audit logs, which may include the user's name and email address.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

The FAA tries to ensure registrants have the information to be knowledgeable of the need for the MyAccess web application and the purposes for which FAA collects, maintains, and

[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

shares PII as part of the identity proofing and MyAccess account registration processes. Individuals requiring access to a FAA application will be advised of their need to register with MyAccess to validate their identity on the takeoff page of that application.

MyAccess registration and account records are maintained in accordance with the Department's Privacy Act system of records notice (SORN), DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002). Accordingly, a Privacy Act Statement discussing the Department's privacy practices regarding the collection, use, sharing, maintenance, and disposal of PII is included on the homepage of the MyAccess web portal. Information maintained in the MyAccess registration records (e.g., name, mobile phone number, email address, and employer information) may be used to authenticate and verify a user's authorized access to an application supported by MyAccess.

Additionally, non-credentialed external users who are U.S. citizens are directed to login.gov and the separate login.gov identity verification process. Login.gov is owned by the General Services Administration and has its own web page that provides a Privacy Act Statement, along with Messaging Terms and Conditions, and Rules of Use.

The publication of this PIA also demonstrates DOT's commitment to providing appropriate transparency into the MyAccess web application.

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.

Users have full access to update and maintain their MyAccess profile information. Additionally, information maintained in MyAccess account registration and system access information is protected under the Privacy Act and individuals may seek access to those records. Individuals may make their inquiries in person or may submit their request in writing to:

Federal Aviation Administration - Privacy Office

800 Independence Avenue (Ave)

SW Washington, DC 20591

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 request in writing, detailing the reasons for why the records should be corrected and addressing their letter to the following address:

Federal Aviation Administration - Privacy Office

800 Independence Avenue, SW

Washington, DC 20591

For foreign nationals who need access to FAA systems or resources, they are required to create an account via login.gov and then have their identity verified by ID Data Web via Application Programming Interface (API) with MyAccess. Identity proofing occurs via an ID Data Web Servers. Foreign Nationals directly provide their PII to ID Data Web via a secure sockets layer.

Neither the FAA nor the ID Data Web maintain the data provided by the individual for identity proofing purposes and therefore do not offer processes for access or correction of this data. If the individual believes that the eID process failed due to erroneous data in the authoritative sources used by the ID Data Web, the individual is encouraged to contact the data owners for their specific guidelines to correct errors (e.g., contact mobile phone provider to confirm the correct name and address are on file). In addition to aiding with identity verification, the FAA may use a registrant's email address and phone numbers to communicate with the registrant for such purposes as automating account resets or other necessary communications.

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.

MyAccess collects information for the purpose of account registration and identity proofing, to ensure that individuals who access FAA network, systems, or applications are who they say they are. In accordance with its statutory responsibilities under 49 U.S.C. 44701(a)(5), 44702 (a)(2), 44703 (b)(B), NIST guidance, and Executive Orders, FAA complies with information security standards and guidelines, including minimum requirements for federal information systems (except for national security systems). NIST Special Publication (SP) 800-63-3 advises that for identity proof – to address impersonation of claimed identity – documentation that provides a specified level of confidence or assurance of the identity of

the person should be used. Government-issued documents such as driver's licenses and passports are examples provided of information to be collected for identity proofing.

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.

Individuals registering accounts with MyAccess and using the eID process are responsible for the accuracy of information they provide during those processes. The data elements collected by the FAA and shared with the IdSP are the minimum necessary to comply with the NIST standards for eID. Information collected for MyAccess account registration and profile maintenance is the minimum required to establish unique accounts within the system, ensure appropriate access to applications, and maintain communications with registered individuals.

MyAccess registration profiles and records associated with the use of MyAccess to access applications will be retained and disposed of in accordance with the applicable record retention schedules. Audit logs generated for information technology operations and system oversight are retained for system administration and destroyed when no longer needed for business operations (GRS 3.1, Item 020). Login information, which includes authentication logs created when users access the system, is destroyed as soon as immediate operational or security monitoring needs conclude (GRS 3.2, Item 030). Routine administrative reports and temporary operational files are categorized as transitory records and are destroyed when no longer needed (GRS 5.1, Item 010). Finally, PIV card and credential records created during the personal identity badge issuance process are temporarily retained and destroyed 6 years after an employee or contractor's tenure ends (GRS 5.6, Item 120).

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.

Sharing of Privacy Act records collected, used, and maintained as part of MyAccess registration account is done in accordance with Department SORN DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002). In addition to other disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

• To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.

• To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.

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

• To other government agencies where required by law.

The Department has published 15 additional routine uses applicable to all DOT Privacy Act SORNs, including this system. The routine uses are published in the Federal Register at 75 FR 82132 (December 29, 2010) and 77 FR 42796 (July 20, 2012), under "Prefatory Statement of General Routine Uses" available at www.tranpsportation.gov/privacy.

Information collected for the eID process is not maintained by the FAA or the IdSP and is used for the limited purposes of conducting identity-proofing activities. The information in records maintained or accessed by the IdSP to validate identities is not accessible by the government and is therefore not covered by the Privacy Act.

For information regarding how login.gov information is used, please view the applicable documentation available on the login.gov Privacy and Security 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).

The individual is responsible for the accuracy of the information they provide during MyAccess registration process. When a new user is registering, they can validate or edit the personal information they have entered prior to proceeding with their registration. Once MyAccess registration is complete, the individual can change their profile information as well as their security PIN and security questions as needed.

The FAA makes no claims that the data obtained and used for identity verification is accurate or complete. Nevertheless, if an individual believes he or she is unable to authenticate his identity due to inaccurate information accessed by the IdSP for identity proofing, the individual is advised to check their information at the various credit bureaus.

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 NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated December 2020.

MyAccess securely transmits information provided by the registrant as described in a prior section of this document to the IdSP using a secure sockets layer (SSL) connection. FAA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII
- Protect against any reasonable anticipated threats or hazards to the security or integrity of PII
- Protect against unauthorized access to or use of PII

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's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division is responsible for governance and administration of FAA Order 1370.121B, FAA Information Security and Privacy Program and Policy. FAA Order 1370.121 implements the various privacy requirements based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), FISMA, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information and information technology management procedures and guidance. The permission rights to MyAccess are based upon role-based access controls, which are granted by automation features as managed and overseen by the FAA. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to the protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy

data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of MyAccess with the requirements of OMB Circular A-130.

Responsible Official

Jeff Adam
9-NATL-MyAccess@faa.gov

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.11.06 15:51:56 -05'00'