U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Information & Technology Services (AIT)

MyAccess Electronic Identity Authentication

Responsible Official

Steven Nichols
Email: steven.nichols@faa.gov
Phone Number: 202-267-3458

Reviewing Official

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

Executive Summary

The MyAccess Electronic Identity Authentication (eID) Service provides identity management and authentication of non-Department of Transportation (DOT)-affiliated individuals requiring access to DOT and Federal Aviation Administration (FAA) applications on the FAA network. The eID services for MyAccess are provided through a third-party service provider (IdSP).

This Privacy Impact Assessment (PIA) is published in accordance with the E-Government Act of 2002 because the new MyAccess capabilities for identity proofing and credentialing require individuals, including members of the public, to provide sensitive personally identifiable information (SPII). The FAA Office of Finance and Management (AFN) Office of Information and Technology Services (AIT) is accountable for the oversight and management of MyAccess.

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 DOT or FAA enterprise networks.[2]

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," the FAA has contracted with a third-party identity proofing services provider (IdSP) to integrate that capability into MyAccess. 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."

The MyAccess program consists of four services that support the DOT and FAA, which are Workforce, Customer Identity and Access Management (CIAM), Identity Confidence Scoring, and Hardware Security Modules (HSM). MyAccess is an Identity and Access

[2] MyAccess identifies, verifies, and authenticates a user to the FAA environment; it does not authorize a user to login to a particular application supported by MyAccess. Application-level access is determined and authorized by each specific application

Management solution for internal (credentialed), external credentialed, and external non-credentialed users.

MyAccess CIAM, in combination with MyAccess Identity Confidence scoring, provides a simplified sign-on process that is designed to verify the identities of – and authentication for – external non-credentialed users accessing FAA applications. The benefit of this expanded capability is that once an external non-credentialed user creates a MyAccess account, they can utilize the same account information to request authorization for each FAA application leveraging MyAccess CIAM. Below is an explanation of the individuals the MyAccess program serves. Each application that an individual is authorized to log into has (or will have) a separate, corresponding PIA, as required, to reflect that application's interface with MyAccess.

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 OMB MAX to leverage their federated authentication solution. 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, a routing rule set within MyAccess CIAM will redirect the user to OMB MAX based on their agency/department domain, i.e., @us.af.mil or @dhs.gov. The user can choose to authenticate with their agency/department PIV or CAC or email authentication with multifactor authentication established within OMB MAX. On successful authentication, OMB MAX then redirects the user back to MyAccess CIAM with a token verifying authentication. MyAccess CIAM then redirects the user to the protected application as an authenticated user and the application then determines authorization.

External Non-Credentialed User:
External non-credentialed users are members of the public, or U.S. citizens or foreign nationals, 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 moderate or higher security threshold and 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 users may create a MyAccess account by visiting the desired application they intend to access. The target application will redirect the users to the MyAccess CIAM Single Sign-on page (SSO), https://myaccessxtl.faa.gov/. From this location, the external users may select the option to *Register for an external account*. Selecting the option to register for an account will redirect the users to https://myaccessreg.faa.gov/. This link is only accessible from the referring application otherwise a message will be presented instructing the user to try again from the target application. Users will be presented the registration form for either an IAL1 or an IAL2 account depending on the referring application's security rating.

IAL 1 Registration:

1. The user enters first name, last name, optional middle name, and a personal or business email address.
2. The user checks a Captcha option to specify they are not a robot and depending on browser may be prompted to select specific images to verify human interaction.
3. MyAccess verifies that the email address is unique and if so, provisions the user within the MyAccess CIAM user store as an IAL 1 account.
4. The user will receive an email with token link to complete account setup.
5. Selecting the link will redirect them to https://myaccessxtl.faa.gov to setup a password and choose one or more multifactor authentication options, Okta Verify, Google Authenticator, or Fast Identity Online 2 (FIDO2).

IAL 2 Registration SSN Option:

1. The user enters first name, last name, optional middle name and a personal or business email address.
2. The user selects the option to verify identity with the last 4 digits of the SSN.
3. The user checks a Captcha option to specify they are not a robot and depending on the browser may be prompted to select specific images to verify human interaction.
4. MyAccess verifies that the email address is unique and that the account is not already registered as an IAL 2 account.
5. User is redirected to a page hosted by ID Data Web (IDDW) that requires the input of home address, last 4 digits of SSN, date of birth, and mobile telephone number.
    a. None of these data elements are stored by MyAccess nor IDDW.
6. IDDW validates the information against several sources to verify identity.
7. If all data matches except for mobile number does not match to the user's full legal name or home address is not associated with user, then IDDW initiates a stepped-up method of verification by prompting the user with knowledge-based answers associated to the user's residence or credit history.

8. The user is allowed 3 attempts with the SSN option to verify identity. On the third failed attempt, the user is provided the option to perform Government Issued ID verification.
9. On success, user is redirected back to MyAccess.
10. MyAccess provisions the user account within MyAccess CIAM user store as an IAL 2 account.
11. The user will receive an email with token link to complete account setup.
12. Selecting the link will redirect the user to https://myaccessxtl.faa.gov to setup a password and choose one or more multifactor authentication options, Okta Verify, Google Authenticator or FIDO2.
13. If the external user fails IAL 2 verification a message will be presented indicating MyAccess is unable to verify their identity and an account will be provisioned as IAL 1.

IAL 2 Registration Government (including specified foreign) Issued ID:

1. The user enters first name, last name, optional middle name and a personal or business email address.
2. The user selects the option to verify identity with Government Issued ID using mobile phone.
3. The user checks a Captcha option to specify they are not a robot and depending on the browser may be prompted to select specific images to verify human interaction.
4. MyAccess verifies that the email address is unique and that the account is not already registered as an IAL 2 account.
5. User is redirected to a page hosted by ID Data Web (IDDW) that requires the user to enter a mobile number, identify the country associated with the government issued ID and to identify if the ID will be a driver’s license, passport, or identification card.
6. User is sent an SMS message with a hyperlink; the link must be accessed from the mobile phone.
7. User is prompted to take a picture of the front of the ID.
8. User is prompted to take a picture of the back of the ID.
9. User is prompted to take a selfie.
   a. Pictures of the government issued ID and selfie are not stored by MyAccess nor IDDW.
10. The user is allowed 3 attempts with the government issued ID option to verify identity. On the third failed attempt the user is provided the option to perform SSN verification.
11. If the ID capture and selfie is successfully verified by IDDW, the user is redirected back to MyAccess.
12. MyAccess provisions the user account within MyAccess CIAM user store as an IAL 2 account.

13. The user will receive an email with token link to complete account setup.
14. Selecting the link will redirect the user to https://myaccessxtl.faa.gov to setup a password and choose one or more multifactor authentication options, Okta Verify, Google Authenticator or FIDO2.
15. If the external user fails IAL 2 verification a message will be presented indicating MyAccess is unable to verify their identity and an account will be provisioned as IAL 1.

ID Data Web:
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 a registrant's information. The process for enabling identity matching of the registrant's information includes:

- 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 their 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 the Department of Motor Vehicles (DMV) for 24 participating states. In instances in which the driver license number is provided, ID Data WebID Data Web attempts to locate a match of the state and driver's license number provided by the external user against driver records on file with the applicable state DMV.

- 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.

- ID Data Web has an established business agreement with a third-party vendor that contracts with the Social Security Administration (SSA) to receive SSNs. Due to the proprietary nature of the contract between SSA and the vendor, and between the vendor and ID Data, the name of the vendor directly receiving SSN data from SSA is confidential and is therefore unknown to FAA.

In-Person ID Verification:
MyAccess provides an interface (https://inpersonreg.sm.faa.gov/) for the Pilot's Record Database (PRD) so that in-person ID verification can be performed by trusted agents of the FAA. These trusted agents are personnel classified as Aviation Inspectors or support personnel of the PRD program. All other access to in-person ID verification is restricted. This is a single page form that requires the trusted agent to enter the user's first name, last name, optional middle name, and email address. The trusted agent must first view the government issued photo ID provided by the external user to verify their identity. The trusted agent will not keep any identity verification data provided by the external user; accordingly, no copies of this photo ID are maintained by the FAA or within MyAccess. The trusted agent will use their own PIV card to authenticate to MyAccess. The trusted agent submits the user's data and MyAccess verifies the email address is unique. If uniqueness is verified, then MyAccess provisions an account in MyAccess CIAM as an IAL2 account and the user will receive an email with token link to complete account setup. Selecting the link will redirect the user to https://myaccessxtl.faa.gov to setup a password and choose one or more multifactor authentication options, Okta Verify, Google Authenticator, or FIDO2.

MyAccess only facilitates access; it does not determine a user's privileges on applications supported by MyAccess. Once the MyAccess account registration process is completed, the individual may be required to complete additional application-specific registration steps for the FAA application for which they are seeking access. These processes are not addressed in this document; however, they are addressed in application specific PIAs as appropriate. All Departmental PIAs may be found on the Departmental Privacy Program website, www.transportation.gov/privacy.

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*

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

the Privacy Controls 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.

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 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.

Information provided by individuals as part of the identity-proofing process is not maintained by either the FAA or the IdSP and are therefore do not constitute records subject to the provisions of the Privacy Act of 1974. Databases used by the IdSP to validate identities – based on data provided by individuals seeking access to DOT/FAA applications protected by MyAccess – are not created at the direction of nor accessed or retrieved by the FAA and are therefore not subject to the Privacy Act. Use of these records for FAA sponsored identity-proofing activities do not constitute "matching" as defined by the Privacy Act[5] and do not constitute credit checks per the Fair Credit Reporting Act.

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.

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

[4] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf
[5] https://www.justice.gov/opcl/privacy-act-1974

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.

The FAA uses the MyAccess platform to collect data directly from the individual and submit it to the IdSP for identity proofing. The IdSP compares this information against its own records and records of authoritative sources to which it has access. If the IdSP is unable to confirm the individual's initial data submission, the individual is provided an opportunity to either correct the data or provide additional data.

Individuals who choose not to provide the last 4 digits of their SSN or for whom an SSN submission cannot be verified by the IdSP may opt to provide their driver's license number. The driver's license number is not a perfect substitution for the SSN and results in less accurate identity validation outcomes due to limitations in accessible records. Individuals whose SSN and driver's license information cannot be verified cannot complete the eID process. Similarly, individuals who provide credit card information have three opportunities to have their account information verified. If after three attempts the IdSP is unable to confirm the individual's financial information, the individual will be prompted to enter a phone number (mobile or home) to receive a one-time password. The phone number entered must match the registrant's name. If the phone number provided is not in the registrant's name, the registrant will be notified that the eID process has failed. Additionally, the individual will be unable to complete the eID process if they are unable to successfully answer the confirmation process as described above. For these circumstances where the eID process was not successfully completed, and the individual is seeking access to PRD, the individual will be notified and afforded an opportunity to complete an in-person identity validation interview and the MyAccess registration process.

Neither the FAA nor the IdSP maintain 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 IdSP, 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.

Individuals 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 inquires 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.

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), and 49 CFR 10.29, and NIST guidance, 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 NARA's General Records Schedule (GRS) 3.2 ''System access records.'' The guidance instructs, ''Temporary. Destroy 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.

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.

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 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.[6]

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.

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 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

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.

[6] http://www.consumer.ftc.gov/articles/0155-free-credit-reports

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

Steven Nichols
MyAccess System Owner

Approval and Signature

Karyn Gorman
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer