U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration (FAA)
Office of Environment and Energy (AEE)
Aviation Environmental Design Tool (AEDT)

Responsible Official

Joseph DiPardo
Email: aedt-support@dot.gov
Phone Number: 202-267-3576

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) Office of Environment and Energy (AEE) developed the Aviation Environmental Design Tool (AEDT) to estimate the environmental consequences of aviation actions, such as noise, fuel consumption, and air pollutant emissions, to help the FAA comply with the National Environmental Policy Act of 1969 (NEPA). AEDT operates under the authority of 42 United States Code (U.S.C.) Chapter 55 - National Environmental Policy; 40 Code of Federal Registry (C.F.R.) Chapter 5, Council on Environmental Quality; and FAA 1050.1F, Environmental Impacts: Policies and Procedures.

The FAA developed this Privacy Impact Assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002 because the AEDT collects Personally Identifiable Information (PII) such as business contact information from members of the public (e.g., environmental analysis consultants, airport operators, academia, and aviation original equipment manufacturers), including foreign users outside of the United States (U.S.). Additionally, because AEDT is available to the public and anyone can open an account and download AEDT, PII may also be collected from individuals who are not associated with an organization/company.[1] Lastly, the system collects PII from DOT/FAA employees and contractors who manage the system.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[2]

[1] Given the nature of the AEDT software, it is unlikely that anyone other than a consultant/company or researcher/university would want AEDT, but the program wants to cover all bases since it is available to all individuals.

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

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 National Environmental Policy Act of 1969 (NEPA) requires federal agencies to consider the environmental impacts of their decisions such as granting permits and constructing publicly owned facilities (e.g., airports). To address NEPA, the FAA developed a downloadable application called the Aviation Environmental Design Tool (AEDT), which provides information on specific environmental impacts. AEDT provides this information to the FAA, aviation entities, and individuals, and operates under 42 U.S.C. Chapter 55-National Environmental Policy; 40 C.F.R. Chapter 5, Council on Environmental Quality; and FAA 1050.1F, Environmental Impacts: Policies and Procedures.

AEDT is comprised of three parts:

1) An application that models how aviation practices affect fuel consumption, emissions, noise, and air quality (AEDT Application). For example, changing a flight path to avoid a populated area could reduce noise in the area but increase fuel consumption.
2) A website that advertises the AEDT Application to companies, federal agencies, and other organizations, including individuals, and provides technical support for the AEDT website.
3) The AEDT Master License Spreadsheet.

Purchasing & Accessing the AEDT Application

Anyone can visit the AEDT website and learn about the AEDT Application without providing PII. However, to purchase the AEDT Application, at least one employee from each business must provide business contact information and PII. Other employees may

provide business contact information and PII if they want to use certain technical support features. Individuals not associated with a company or organization provide their PII to purchase the AEDT Application and must take the same actions as a company or organization takes to purchase and access the AEDT application as detailed below.

The AEDT website's Pricing Page explains the steps a business or individual must take to purchase the AEDT Application:

1. A business' employee or individual visits EUROCONTROL's Base of Aircraft Data (BADA) website and applies for a BADA license. EUROCONTROL is a Europe-based intergovernmental organization focused on managing air traffic within Europe. BADA is EUROCONTROL's database of aircraft information that employees or individuals must install to use the AEDT Application. If EUROCONTROL approves the application, they send the employee or individual, and the AEDT Support Team,[3] an email containing the employee's or individual's name, business or personal contact information, and approval. The AEDT Support Team records this on a shared drive and then deletes the email.[4]
2. An employee or individual visits the AEDT website Registration Page and request an AEDT website account. This process collects the business point of contact (POC) name, organization name, business address, business phone number, and business email address, username, password, security question and answer. If an individual is purchasing the software, they enter their personal including address, phone number, and email address, username, password, and security question and answer. Once the AEDT Support Team receives an email from EUROCONTROL that says the business or individual has a BADA license, the team activates the account and informs the employee or individual via email.
3. The employee or individual with the AEDT website account logs in and clicks the Pay.Gov link, which is a payment-processing website run by the Department of the Treasury.[5] If the payment is successful, Pay.Gov sends the employee and the AEDT Support Team an email containing the employee's name, business contact information, and amount paid. If it is an individual, Pay.Gov sends the individual and the AEDT Support Team an email containing the individual's name, personal contact information, and amount paid. The AEDT Support Team records the information on a shared drive, deletes the email, then sets the AEDT website so the employee/individual can download the software.

[3] The AEDT support team is responsible for the AEDT Operations and Maintenance (O&M) support website application, which exists so that AEDT software users can submit bug reports and receive feedback from the AEDT software development team via the support website.
[4] EUROCONTROL provides a User Guide that further explains the application process.
[5] Please see the Pay.Gov SORN FS. 013 – Collections Records – 85 FR 11776 (Feb. 27, 2020) and PIA for more information on its functions and privacy implications.

4. The employee or individual with the AEDT website account returns to the AEDT website, downloads the software, and installs it.

Requesting Support for the AEDT Application

Once a business has access to AEDT, all other employees can choose how they want to interact with the AEDT website and AEDT Support Team. Employees who create their own AEDT website account can (1) access additional information about AEDT Application, (2) send feedback to the AEDT Support Team and receive responses, (3) view all feedback submitted by other employees with accounts, and (4) access the link to Pay.Gov where they can purchase technical support and additional AEDT licenses. Creating that account requires the employee to provide their name and business contact information, username and password, and security question and answer. Individuals wishing to ask general questions or provide feedback can send an email to the address posted on every page of the AEDT website. That requires an email address and, depending on the request, an AEDT Application license number. Individuals not associated with a business may purchase and use the software. They provide personal information for this process.

FAA Tracking of Licenses

The internal AEDT Master License document is an Excel spreadsheet file located on a shared drive, accessible only to the AEDT Support Team. The spreadsheet includes a list of all entities that purchase the AEDT Software, information about a POC for each entity, what each entity purchased (e.g., software licenses and technical support), and what purchases have been fulfilled. This spreadsheet is encrypted, and password protected.

The Master License Spreadsheet maintains the following user provided data: name of the business POC, organization name, business address, business phone number, and business email address. If an individual is not associated with a business, but wants to purchase and use AEDT, the Master License Spreadsheet maintains the individual's name, address, email address, and phone number.

The AEDT Support Team accesses the data included in the spreadsheet by running search queries using date ranges. The AEDT Support Team members do not search for, or retrieve, records using a personal identifier of any individual. Substantive records are only retrieved when users create a ticket to report a software bug or require user support. Records are retrieved by ticket number or by subject, never by name, username, or any other PII element.

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[6].

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 AEDT website is a privacy-sensitive system because it maintains collects, uses, disseminates, and retains PII from members of the public (e.g., environmental analysis consultants, airport operators, academia, and aviation original equipment manufacturers), including foreign users outside of the United States (U.S.), for creating and managing AEDT accounts. Policies, procedures and practices for information storage, data use, access, notification, retention and disposal are described herein this PIA.

The FAA deploys multiple techniques to inform individuals why the FAA collects, uses, disseminates, and retains PII within AEDT. The records in AEDT regarding the purchasing and support of licenses are not retrieved by PII, and thus, are not covered under the Privacy Act and, therefore, no System of Records Notice (SORN) coverage is required. The FAA uses access information for the purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the AEDT 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).

For account management, the AEDT website collects all PII directly from the employee. Once the AEDT Support Team approves an employee's request for a new AEDT website account, they can login to the website at any time to view and update their information. Every page of the AEDT website includes a link to the AEDT website Privacy Policy, which explains what PII is collected, how it is used, where it is shared, and how it is protected. It also invites individuals to contact the AEDT Support

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

Team if they have questions, which includes any questions about the Privacy Policy or their PII.

When a company's employee requests a BADA license or makes a payment through Pay.Gov, a confirmation email with their name and business contact information goes to the AEDT Support Team. The employee will know this occurred because they receive a copy of the email.

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) on the access form, and at the point of collection for individuals when they request an access form from whom the program collects PII, that details the purpose and authority to collect PII as well as the routine uses of the PII.

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

As noted above, the AEDT website collects all PII directly from the individual, and once the individual's request for a new AEDT website account is approved, they can login to the website at any time to view and update their information, except for their email address. If they want to change their email address, they can create a new account and contact support to transfer their license to the new account. Because the information was collected directly from the individual, it is expected to be accurate.

Under the provisions of the Privacy Act, individuals may request searches of the AEDT system to determine if any records have been added that may pertain to them and if such records are accurate.

For all inquiries related to the information contained in the AEDT website, the individual may appear in person, send a request via email (privacy@faa.gov), or in writing to:

Privacy Office
800 Independence Avenue, 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
- A signed attestation of identity

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 develop systems and/or tools to facilitate environmental review activities required under NEPA. The AEDT addresses the unique demands of the FAA's workforce and operates under the authority of:

- 42 U.S.C. Chapter 55 - National Environmental Policy: This chapter is the NEPA that requires federal agencies to consider the environmental impact of certain decisions such as granting permits and constructing publicly owned facilities. It also created the Council on Environmental Quality (CEQ) and gave CEQ the power to establish guidance on how federal agencies should comply with NEPA.
- 40 CFR Chapter 5, Council on Environmental Quality: This chapter further explains how federal agencies must operate in order to comply with NEPA.
- CEQ Guidance: This website contains guidance from CEQ on how federal agencies must operate in order to comply with NEPA.
- FAA 1050.1G, National Environmental Policy Act Implementing Procedures: This FAA Order establishes how the FAA will comply with NEPA.

The AEDT website maintains the following PII on federal employees and contractors to manage the AEDT software and program, and for authentication and access. The AEDT website collects federal employee and contractor name, username/email address, title, branch, role, and office.

The FAA uses this 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 AEDT 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).

In addition, the AEDT website maintains the following PII on members of the public (environmental analysis consultants, airport operators, academia, aviation original equipment manufacturers, and individuals):

- Business or Personal Email Address if not associated with an organization/company
- Organizational Users/Payers/Point of Contact (POC) Name (which could be an individual's name if not associated with an organization/company)
- Business Mailing Address or Personal Mailing Address (if not associated with an organization/company)
- Country
- Business Telephone Number or Personal Telephone Number (if not associated with an organization/company)
- Transaction Amount

The AEDT website uses this information in accordance with the purposes for which it is collected:

1. Distribute the AEDT Application.
2. Confirm that the users have the BADA license needed to use the AEDT Application.
3. Confirm that the users have paid for software and technical support services.
4. Respond to user questions about the software.
5. Notify users about software changes.
6. To reset user's password upon request.

AEDT is not a Privacy Act system of records for the substantive records regarding the purchasing and support of licenses and thus no System of Records Notice (SORN) is required. However, the FAA maintains user account access information and those records are handled in accordance with DOT/ALL 13, *Internet/Intranet Activity and Access Records,* 67 FR 30757 (May 7, 2002).

The PII in the AEDT 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 individuals to support the FAA's AEDT website user access and usage. The exact amount of PII collected from each individual depends on how those individuals choose to interact with AEDT.

AEDT Support reviews the user account information provided and redacts any unnecessary PII before activating the user account to allow purchase and download of AEDT software.

The AEDT website's Pricing Page advises individuals to make sure their business has a BADA license from EUROCONTROL before requesting an AEDT website account. The AEDT website will not allow individuals to purchase the AEDT Application until they show that their business has acquired a BADA license. This is because both of those transactions are unnecessary if the business cannot acquire a BADA license.

Individuals, including those not associated with a company, who purchase and download AEDT,0 can decide how much PII they want to provide:

- Those who want to benefit from all AEDT website features must create an account via the AEDT website's Registration Page. Creating that account only requires a name and contact information, a username and password, and a security question and answer.
- Those who want to email the AEDT Support Team about an issue can use the email, aedt-support@dot.gov, which is posted on every page of the AEDT website. These communications only require individuals to provide their email and, depending on the request, an AEDT Application license number.

The AEDT website allows employees to submit feedback and states, both above and below the text fields, that the title and description of the feedback will be visible to others with accounts. It also explains that employees should upload feedback as an attachment if they only want the AEDT Support Team to see it.

The FAA maintains different types of records in accordance with following National Archives and Record Administration (NARA) approved General Retention Schedules[7] (GRS):

- Audit logs are cutoff when account activity is finalized and destroyed 3 year(s) after cutoff. AEDT Reports, including the Internal AEDT Master License, are destroyed 3 years after cutoff (cutoff occurs at the end when reports are reconciled).[8]
- Non-substitutive records in AEDT including login credentials, audit trails, and security monitoring are retained until the business no longer needs the records.[9]
- Information Technology Operations and Maintenance Records are destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is

[7] 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.
[8] DAA-0237-2020-0023, Aviation Environmental Design Tool (AEDT).
[9] NARA GRS 3.2, *Information Systems Security Records, System Access Records*, approved January 2023, Item 031.

obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.[10]

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 the AEDT website collected from environmental analysis consultants, airport operators, academia, aviation original equipment manufacturers, and individuals is used to/for:

- Reply to feedback and technical support inquiries;
- Send notices about new software and documentation;
- Personalize one's experience;
- Allow access to restricted areas of the AEDT website;
- Address security or virus threats;
- Purposes of law enforcement or national security; and
- Other purposes required by law.

The FAA does not use the PII for any other purpose.

Access and authentication records within the AEDT website are handled in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002). As such, all or a portion of the records or information contained in AEDT may be disclosed outside of DOT as a routine use pursuant to 5 U.S.C. § 552a(b)(3) to:

- 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.

[10] NARA GRS 3.1, *General Technology Management Records*, approved November 2019, Item 20.

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" and include, but are not limited to:

- In the event that a system of records maintained by DOT to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto.
- A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DOT decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.
- A record from this system of records may be disclosed, as a routine use, to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

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).

All PII collected by the AEDT website is presumed accurate since it is collected directly from the AEDT users (organization/company employees or an individual not associated with an organization/company). Once the AEDT Support Team approves a user's request for a new AEDT website account, the user may log into the website at any time to view and update their PII. If an individual creates a new account that the AEDT Support Team has not yet approved, or has another issue with the AEDT website, they can contact the AEDT Support Team for assistance via the email posted on every page of the website.

All PII collected by the AEDT Support Team from the EUROCONTROL and Pay.Gov is presumed to be accurate since it is collected from the individual. If the same individual completes both processes, the AEDT Support Team uses the PII in the Pay.Gov email to confirm that the information captured from the EUROCONTROL email is accurate. If there is a discrepancy, then they are not granted access. Typically, if an employee leaves their organization, the AEDT Support team is contacted to transfer their license to a different employee at the same organization. Also, when AEDT email notices are sent, the AEDT Support team takes note of any emails that are returned to the sender due to undeliverable addresses. AEDT users can update their information in their user profile on the support website at any time. Sometimes a user changes their email address and the AEDT support team is contacted to disable their old account and transfer their license to the new email account (which could happen if a user changes their name, for example).

The AEDT Support Team developed an incident response plan so all AEDT Support Team members know when and how to report a problem with the AEDT website, such as a malfunction that affects PII, and how AEDT Support Team members should work to remediate concerns. The AEDT website creates an audit log of unusual activities, and the AEDT Support Team members routinely review those logs and investigate any concerns.

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 the AEDT website 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 the AEDT website. 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 the AEDT website 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.

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 the AEDT website are given clear guidance about their duties as related to collecting, using, and processing privacy data.

Clear guidance is provided to federal and contract employees via mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of the AEDT websites related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Joseph DiPardo
System Owner
Operations Research Analyst, Office of Policy and Strategic Engagement (APL)

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2025.12.11 16:51:50 -05'00'