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
Acting Chief Privacy & Information Asset Officer
Office of the Chief Information Officer (OCIO)
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).

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.). PII is also collected from individuals who are not associated with an organization/company. In addition, 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.[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;*

[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).

- *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 impact of 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.

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, how changing a flight path to avoid a populated area could reduce noise in the area and 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/PII for that business. Other employees may provide business contact information/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 employee or individual must install to use the AEDT Application. If EUROCONTROL approves the application, they send the employee (or individual) and the AEDT Support Team[2] an email containing the employee/individual name, business or personal contact information, and approval. The AEDT Support Team records that on a shared drive and then deletes the email.[3]

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, and 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 have a BADA license, the team activates the account and inform 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.[4] 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 that information on a shared drive, deletes the email, then sets the AEDT Website so the employee/individual can download the software.

4) The employee or individual with the AEDT Website 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

[2] 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.

[3] EUROCONTROL provides a User Guide that further explains the application process.

[4] Please see the Pay.Gov System of Records Notice and PIA for more information on its functions and privacy implications.

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[5]*, 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*

[5] 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[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 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. FAA maintains the user access account information and those records are handled in accordance with 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 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.

Lastly, the publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency into AEDT, and to provide notice to the public as to the information management policies and practices related to this 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

[6] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

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.

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. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

AEDT operates under the following authorities:

- 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 1050.1F, Environmental Impacts: Policies and Procedures: This FAA Order establishes how the FAA will comply with NEPA.

The AEDT Website collects the company name, company POC name, business mailing address, business email address, business telephone number, username/password, and security question and answer from AEDT users, including individuals not associated with a company for the following:

(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.

The AEDT Support team collects PII from DOT/FAA employees and contractors to manage the software and program and for authentication and access.

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).

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.

AEDT collects the minimum amount of PII necessary to support the user's access and usage of AEDT. 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 acquired a BADA license. This is because both those transactions are unnecessary if the business cannot acquire a BADA license.

Individuals, including those not associated with company, who purchase and download AEDT 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.

Substantive records in the system are handled in accordance with the National Archives and Records Administration (NARA) record schedule, DAA-0237-2020-0023. The FAA destroys audit logs 3 years after business use ceases. AEDT Reports, including the Internal AEDT Master License, is destroyed 3 years after cut off (cut off occurs at the end when reports are reconciled).

Non-substitutive records in AEDT including login credentials, audit trails, and security monitoring are retained until business use ceases in accordance with NARA GRS 3.2, September 2016, *Information Systems Security Records*, System Access Records.

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 collected through the AEDT Website is in accordance with the AEDT Website Privacy Policy and may be used for the following:

- To reply to feedback and technical support inquiries;
- To send notices about new software and documentation;
- To personalize one's experience;
- To allow access to restricted areas of the AEDT Website;
- To address security or virus threats;
- For purposes of law enforcement or national security; and
- For other purposes required by law.

PII stored in the AEDT website is only available to (1) the person who provided that PII and (2) members of the AEDT Support Team.[7] The AEDT senior management assure that only those team members who need access to the PII have that access. Each team member signs a Rules of Behavior document before receiving access and completes privacy and security training on an annual basis. Every time team members access the administrative part of the AEDT Website and may view PII, they must first agree to only use and disclose that PII for a U.S. Government-authorized purpose and acknowledge that any violation may lead to disciplinary actions, civil penalties, and criminal penalties.

PII captured from the EUROCONTROL and Pay.Gov emails are stored on a shared drive that only the AEDT website team can access. The AEDT website team consists of the AEDT Project Manager leads and the AEDT Emergency Response Team who coordinate with the AEDT System Admin, the FAA System Owners, and the Volpe Center IT team. The team stores this information because both the FAA and the vendor who developed the software

[7] The AEDT support team consists of the AEDT Project Manager leads and AEDT O & M team, which also includes the AEDT Subject Matter Expert and development team, as needed.

underlying the AEDT Application want to track the number of organizations/companies that purchased the software and how many copies of the software they purchased.

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

Substantive records in the system are not covered under the Privacy Act because they are not retrieved by personal identifier. Access and authentication records within AEDT are handled in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002).

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 returned as 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

The AEDT Website employs administrative, technical, and physical measures to protect PII against loss, unauthorized access, or disclosure. All PII is encrypted when transmitted. All individuals with an AEDT Website account must set a complex password and their account locks if they do not change that password every 90 days. They also agree to report events or incidents that may compromise their AEDT account. AEDT Support Team members with access to PII receive clear guidance in their duties as they relate to collecting, using, processing, and securing privacy information. This guidance includes mandatory annual security and privacy awareness training, as well as Rules of Behavior. The DOT and FAA Privacy Office will conduct periodic privacy compliance reviews of the AEDT Application and AEDT Website with the requirements of OMB Circular A-130.

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 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,) the FISMA, DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, additional policies and procedures are consistently applied, especially as they relate to the access, 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 security privacy information. 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 conduct annual privacy compliance reviews, i.e., Privacy Threshold Assessments (PTA) or Privacy Continuous Monitoring (PCM) of the AEDT program relative to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

The AEDT Website creates an audit log of unusual activities and members of the AEDT Support Team routinely review those logs and investigates any concerns.

Responsible Official

Joseph DiPardo
System Owner
Operations Research Analyst
Office of Policy, International Affairs and Environment (APL)

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

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