U.S. Department of Transportation

Federal Aviation Administraiton (FAA)

Privacy Impact Assessment
Service Availability Prediction Tool (SAPT)

Responsible Official
David E. Gray
Program Manager
David.E.Gray@faa.gov

Approving Official
Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2020.01.30 10:01:44 -05'00'

Executive Summary

On May 28, 2010, the Federal Aviation Administration (FAA) published the Automatic Dependent Surveillance – Broadcast (ADS-B) final rule mandating that aircraft flying in certain controlled airspace be equipped with ADS-B Out capability not later than January 1, 2020.[1] In turn, the FAA developed the Service Availability Prediction Tool (SAPT) to assist pilots, dispatchers, and commercial operators in checking their predicted navigation and surveillance availability before a flight as well as handle requests for Air Traffic Control (ATC) authorization pursuant to 14 CFR § 91.225(g). The SAPT has three main components: Receiver Autonomous Integrity Monitoring (RAIM) SAPT, Automatic Dependent Surveillance-Broadcast (ADS-B) SAPT, and ADS-B Deviation Authorization Pre-Flight Tool (ADAPT). This Privacy Impact Assessment (PIA) was developed pursuant to Section 208 of the E-Government Act of 2002 because the SAPT includes a web-based capability to collect and manage Personally Identifiable Information (PII) captured from aircraft operators to facilitate the automated handling of ATC authorization requests and FAA's responses.

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]

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

DOT Privacy Office - Approved 01/2020

[1] See (Federal Register/Vol. 75, No. 103), available at https://www.govinfo.gov/content/pkg/FR-2010-05-28/pdf/2010-12645.pdf.

[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).

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 Federal Aviation Act of 1958 gives the Federal Aviation Administration (FAA) responsibility for carrying out safety programs to ensure the safest, most efficient, aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety
- Encouraging and developing civil aeronautics, including new aviation technology
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation, and
- Regulating U.S. commercial space transportation

As part of this effort, the FAA published the Automatic Dependent Surveillance Broadcast (ADS-B) Out Performance Requirements to support Air Traffic Control (ATC) Service Final Rule on May 28, 2010 (75 FR 30159). The ADS-B Out Final Rule requires that an aircraft be outfitted with ADS-B Out equipment to operate in Classes A, B, and C airspace, as well as other specified classes within United States airspace.

ADS-B Out Overview:

Automatic Dependent Surveillance–Broadcast (ADS-B), is a surveillance technology that helps pilots and air traffic controllers create a safer, more efficient National Airspace System (NAS). ADS-B improves safety and efficiency in the air and on runways, reduces costs, and lessens harmful effects on the environment. ADS-B is an environmentally friendly

DOT Privacy Office - Approved - 013020

technology that enhances safety and efficiency, and directly benefits pilots, controllers, airports, airlines, and the public. ADS-B Out relies on aircraft avionics, a constellation of Global Positioning System (GPS) satellites, and a network of ground stations across the country to transmit an aircraft's position, ground speed, and other data to air traffic controllers. Its coverage area and position accuracy are greater than that of radar and can also be used as a more cost-effective surveillance solution in remote areas such as over the Gulf of Mexico or in certain mountainous regions. ADS-B installed avionics continuously transmit aircraft information through 1090-megahertz (MHz) extended squitter (ES) broadcast link or the Universal Access Transceiver (UAT) broadcast link to be received by the FAA via automation, for use in providing air traffic surveillance services. ADS-B equipment will periodically broadcast information about an aircraft's GPS location, International Civil Aviation Organization (ICAO) aircraft address and aircraft identification, in "real time" to FAA ground receivers. Air traffic controllers and aircraft equipped with ADS-B In can immediately receive this

longitudinal separation standards.

The FAA's Surveillance and Broadcast Services Program Office manages ADS-B services in the NAS. Beginning January 2, 2020, the U.S. will require aircraft operating within designated airspace to be equipped with ADS-B Out (see 14 CFR §§ 91.225 and 91.227). Section 91.225 prescribes the ADS-B Out equipment and use requirements, and Section § 91.227 prescribes the ADS-B Out equipment performance requirements. Section 91.227 specifies ADS-B equipment performance requirements. The ADS-B Out rule does not dictate using a specific type of GPS receiver, but the achieved performance depends on the type of GPS receiver that is used as the ADS-B position source. After January 1, 2020, unless otherwise authorized by ATC, all aircrafts operating in the airspace identified in 14 CFR § 91.225 must comply with the ADS-B Out equipage and performance requirements specified in 14 CFR §§ 91.225 and 91.227.

The FAA adopted a provision in 14 CFR § 91.225(g), that allows operators to request authorization from ATC to operate in ADS-B Out airspace with aircrafts that do not fully

[3] The 2010 final rule only mandated ADS-B Out. However, some aircraft have opted to go beyond the mandate to equip with ADS-B In. ADS–B In refers to an appropriately equipped aircraft's ability to receive and display another aircraft's ADS–B Out information as well as the ADS–B In services provided by ground systems, including Automatic Dependent Surveillance–Rebroadcast (ADS–R), Traffic Information Service–Broadcast (TIS–B), and, if so equipped, Flight Information Service–Broadcast (FIS–B). Information on ADS-B In can be found here: https://www.faa.gov/nextgen/programs/adsb/pilot/.

meet the ADS-B Out requirements. On April 1, 2019, the FAA published guidelines for how ATC will manage 14 CFR § 91.225(g) and issue authorizations to operators of aircrafts that have not installed ADS-B Out equipment but wish to fly in ADS-B Out airspace. The collection of data is required for FAA to handle requests for authorization from operators of aircraft that do not meet the equipage requirements specified in 14 CFR § 91.225.

Service Availability Prediction Tool (SAPT)

The SAPT is an automated internet-accessible suite of tools developed to assist pilots, dispatchers, and commercial operators to check their predicted navigation and surveillance availability before a flight. The SAPT has three main components: Receiver Autonomous Integrity Monitoring (RAIM) SAPT, ADS-B SAPT, and ADS-B Deviation Authorization Pre-Flight Tool (ADAPT).

The SAPT prediction service is freely available over the Internet. There is no requirement to create a user account or submit PII to access or use the tool (i.e., no user names or passwords are required to use the tool). Announcements regarding changes to the SAPT web service and web site will be made periodically. Anyone, including the intended users, interested pilots, dispatchers, and commercial operators, can subscribe to the SAPT email "Announcement List" at https://sapt.faa.gov/request.php?action=joinlist.

Receiver Autonomous Integrity Monitoring (RAIM) SAPT

The use of RAIM SAPT is voluntary and intended to provide situational awareness for pilots, dispatchers, and commercial service providers using Technical Standard Order (TSO)-C129 equipment to check the availability of GPS RAIM for a proposed route of flight. The RAIM prediction model constructs the GPS constellation from a given almanac. This almanac is usually the most recent, but can also be an historic one, to construct scenarios or for validation. The GPS constellation is iterated over the prediction window using the specified time interval. Using RAIM SAPT satisfies the area navigation (RNAV) guidance as outlined in AC 90-100A Change 2, Paragraph 10a(5)[4]. RAIM SAPT users can graphically view RAIM outage predictions on RAIM Summary Displays for specific equipment configurations. RAIM SAPT predictions are only available through an XML-based web interface. RAIM SAPT users can use the XML-based web service, most commonly used by a flight planning software, to enter a specific route of flight information by the operators checking RAIM outage predictions. RAIM SAPT does not collect PII about the operator(s) however it does provide maps of wide area outages as a flight planning aid.

The RAIM SAPT is exclusively an XML-based web service, most commonly used by flight planning software (including both custom and third-party solutions). If a pilot, dispatcher, or

[4] Operators may choose to monitor the status of each satellite in its plane/slot position, account for the latest GPS constellation NOTAMs, and compute RAIM availability using model-specific RAIM prediction software, or by using the SAPT on the FAA en-route and terminal RAIM prediction Web site, or by contacting a Flight Service Station (FSS).

DOT Privacy Office - Approved: 01020

commercial service provider is using a flight planning software from a third-party vendor, it is recommended that the third-party vendor incorporate the FAA's RAIM SAPT web service into their software. If a pilot, dispatcher, or commercial service provider build and/or maintain their own flight planning software, a copy of the SAPT Software Development Kit (SDK) and the Web Service Description Language (WSDL) file for the SAPT web service is available from the FAA and can be downloaded. The WSDL file is a technical description of the software interface to a web service that programmers can use to write software that can communicate with a web service. The SAPT WSDL allows the SAPT service to be integrated with flight planning software.

Automatic Dependent Surveillance-Broadcast (ADS-B) SAPT

The ADS-B SAPT helps operators comply with 14 CFR §§ 91.225 and 91.227 by predicting whether their proposed aircraft operation(s) will meet regulatory requirements and to advise holders of FAA Exemption No. 12555 on whether back-up surveillance will be available where installed aircraft avionics are not predicted to meet the requirements of 14 CFR §§ 91.227(c)(1)(i) and (iii). For operation of aircraft equipped with TSO-C129 (Selective Availability (SA)-On) GPS receivers, operators may run a preflight prediction using ADS-B SAPT as one option to help meet their requirements. Information collected via ADS-B SAPT (detailed further below) is comparable to that already provided in flight plans, with the addition of some information about the aircraft avionics, i.e. position source's TSO and related capabilities. Operators using the ADS-B SAPT must enter their aircraft identification. The ADS-B SAPT does not collect other PII about operators. When an operator performs a preflight surveillance availability prediction using the ADS-B SAPT, the ADS-B SAPT retains a record of each transaction enabling the FAA to confirm that operators took preflight actions. This transaction record is stored within the FAA's ADS-B Performance Monitor (APM). The FAA recommends that operators using an alternate tool retain documentation that verifies the completion of the satisfactory preflight availability prediction for each intended route of flight.

ADS-B SAPT predictions may be requested using XML or the SAPT "Flight Information Entry" form, which has been modeled after a standard FAA Flight Plan form for ease of use. All the active fields of the "Flight Information Entry" form require aircraft operators to enter relevant data. In addition to direct data entry, the Flight Information Form allows aircraft operators to save and load flight and aircraft information and paste it into an ICAO Flight Plan. The following information is required:

1. Aircraft Identification (or "Call Sign")
2. Aircraft Type
3. ADS-B Position Source TSO (or unequipped)
4. ADS-B link TSO (or unequipped)
5. Proposed Departure Time (UTC)

DOT Privacy Office - Approved - 013020

6. Planned Altitude
7. Departure Airport
8. Destination Airport
9. Route of Flight

In addition to the standard information, the interactive user interface includes the following fields:

- ADS-B Position Source TSO (or "unequipped" or "inoperative") — this is required information
- ADS–B Link TSO (or "unequipped" or "inoperative") — this is required information
- Mask Angle — the default value is 5.0. Select N/A if flight is unequipped with ADS-B, or GPS position source is inoperative.
- Barometric Aiding — this is required information.

ADS-B Deviation Authorization Pre-Flight Tool (ADAPT)

ADAPT is used by aircraft operators who desire to fly an aircraft that is not equipped with ADS-B or that is predicted to not meet the required position performance. ADAPT allows aircraft operators to request an authorization from ATC to deviate from the equipage or performance requirements of 14 CFR §§ 91.225 or 91.227, under certain circumstances. To relieve the potential burden on ATC facilities, the FAA developed the ADAPT to manage aircraft operators' requests for an ATC authorization.

As a requirement for using ADAPT, aircraft operators must first complete the ADS-B SAPT "Flight Information Entry" form to determine if sufficient backup surveillance coverage is available throughout their planned flight in rule airspace.

In addition to the information required for ADS-B SAPT, the following information is required for ADAPT:

1. Name of Pilot in Command (PIC)
2. PIC Telephone Number
3. PIC Email Address
4. Aircraft Identification (U.S. Civil Aircraft Registry Number or ICAO Address (hex, octal or decimal))
5. ADS-B Equipment Status (unequipped, inoperative, insufficient)
6. Working Transponder with Altitude Reporting? Yes/No
7. Affected en-route ATC facilities
8. Flight Classification: Part 91, 121, 129, or 135
9. Reason for Request
10. Certification of Truthfulness

DOT Privacy Office - Approved - 013020

Flight Information Entry Forms

The ADS-B SAPT or ADAPT "Flight Information Entry" form is used by pilots, dispatchers, and commercial operators to enter the specific flight details. ADS-B SAPT will analyze the proposed flight details, and if the aircraft is not predicted to meet the position accuracy requirements of 14 CFR § 91.227, aircraft operators may submit a request to the FAA for an ATC authorization using ADAPT. A non-equipped aircraft will automatically fail the ADS-B portion of the performance prediction, but aircraft operators are still required to first use ADS-B SAPT, because the ADS-B SAPT analysis provides alternate (non-ADS-B) surveillance information that is necessary for evaluating an ATC authorization request.

VADS-B SAPT/ADAPT "Flight Information Entry" forms collect operator information needed for prediction and application process purposes only. Operators information submitted via ADS-B SAPT or ADAPT will not generate, nor should they be considered, formal Visual Flight Rules (VFR) / Instrument Flight Rules (IFR) flight plan submissions.

For additional information about the SAPT and its main components of RAIM SAPT, ADS-B SAPT and ADAPT please visit https://sapt.faa.gov/default.php or email the FAA at sapthelp@faa.gov and adapthelp@faa.gov.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template 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 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].

DOT Privacy Office - Approved-013020

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

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

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.

SAPT does not retrieve records by a unique identifier linked to an individual (rather, records are retrieved using information relating to the aircraft). Additionally, records maintained by SAPT are associated with the aircraft and not an individual. Accordingly, SAPT is not a Privacy Act system of record and no system of record applies.

The FAA used multiple forms of communication to inform aircraft owners, General Aviation (GA) community, dispatchers, commercial operators, and others to assist aircraft operators in achieving compliance with the requirements of 14 CFR §§ 91.103, 91.225, and 91.227. Included in the outreach effort was information that described the SAPT and the main components that fell under the SAPT umbrella: RAIM SAPT, ADS-B SAPT and ADAPT. Also, included in the information outreach was a description of reasons why and how the FAA collects and maintains PII in support of the ADS-B SAPT and ADAPT functions. Outreach efforts included, FAA sponsored speaker events, information posted on FAA websites, and information publicized via Aircraft Owners and Pilot Association, National Business Aircraft Association, General Aviation Manufacturers Association, Aircraft Electronics Association, Equip2020, and other organizations as means to inform aircraft owners and operators.

The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into SAPT and its three main components: RAIM SAPT, ADS-B SAPT, and ADAPT.

Individual Participation and Redress

DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

SAPT uses data collected directly from pilots, dispatchers, and commercial operators specific for checking predicted navigation and surveillance availability before a flight.

Information collected from pilots, dispatchers, and commercial operators using the ADAPT function includes; the aircraft operator's contact information (i.e., name, phone number, and

DOT Privacy Office - Approved - 01/2020

e-mail address) and is used by the FAA to reply with either an approval, rejection, or pending decision.

Pilots, dispatchers, and commercial operators understand that their provided information will be utilized to verify eligibility for an ATC authorization under 14 CFR § 91.225g) and for communicating with DOT/FAA. Records maintained by SAPT are not subject to the Privacy Act.

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 its collects, uses, maintains, or disseminates PII.

Under Title 49 of the United States Code (49 U.S.C.), Subtitle I, Section 106, the FAA is charged with prescribing regulations on the flight of aircraft (including regulations on safe altitudes) for navigating, protecting, and identifying aircraft, and the efficient use of the navigable airspace. Under section 44701, the FAA is charged with promoting safe flight of civil aircraft in air commerce by prescribing regulations for practices, methods, and procedures the Administrator finds necessary for safety in air commerce.

SAPT data and records will be used by the FAA, consistent with the purposes for which they were collected. Specifically:

- Predict whether an aircraft flying the proposed route of flight will have sufficient position accuracy and integrity for:
  - Navigation, via the RAIM SAPT
  - Surveillance, via the ADS-B SAPT
- Allow operators to request authorization, via ADAPT, from ATC to operate aircrafts that do not fully meet ADS-B Out equipage or performance requirements (per 14 CFR §§ 91.225 and 91.227), in airspace that requires ADS-B Out (per 14 CFR § 91.225).

The name, phone number and email address collected in the ADAPT application is used by the FAA to respond with an official email with the status of the ADAPT application. The official email to the aircraft operator will be either an approval, rejection, or pending decision. In the case of a pending status, the requestor will receive an immediate email response stating the pending status. A second email will be sent later, once the request has been adjudicated by ATC and has been approved or denied. Operators are encouraged to retain FAA's approval email for any flight.

DOT Privacy Office - Approved - 01320

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only if necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The FAA collects the minimum amount of information necessary (only the name, phone number, and email addresses of aircraft operators) to establish and maintain a record to support the aircraft operators using pre-flight availability predictions for navigation and surveillance, and for submitting a request for an authorization as required by 14 CFR § 91.225 paragraph (g) from ATC. The name, phone number and email address is used by the FAA to communicate the approval, rejection or pending decision with aircraft operators.

Records for the SAPT will be maintained as permanent records until FAA receives an approved disposition authority from the National Archives and Records Administration (NARA). The proposed retention periods are outlined in DAA-0237-2020-0002. The SAPT application that includes the name, phone number and email is maintained temporarily and will be destroyed no sooner than two years, but longer retention is authorized. The retention period will allow the FAA to facilitate and maintain a history of the ATC authorization request and FAA response.

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.

SAPT information is used to assist pilots, dispatchers, and commercial operators in checking their predicted navigation and surveillance availability before a flight as well as handle requests for ATC authorization pursuant to 14 CFR § 91.225(g). There is no internal sharing of the information collect by SAPT.

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).

FAA collects the name, phone number and mail address directly from the aircraft operator. The information is used to communicate the approval, rejection or pending decision with the aircraft owner. The aircraft operators are asked to review their information for accuracy prior to submitting their request.

DOT Privacy Office - Approved 01/2020

Security

DOT shall implement administrative, technical, and physical measures 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.

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.

SAPT was issued a three-year Authorization to Operate (ATO) in September 2018. The SAPT web application will be evaluated in annual security review cycles. In addition, the ATO will be updated based on the outcome of current security testing and evaluation in accordance with FISMA. Access to the SAPT application is limited to those with appropriate security credentials, an authorized purpose, and need to know. The FAA deploys role-based access controls in addition to other protection measures reviewed and certified by the FAA's cybersecurity professionals to maintain the confidentiality, integrity, and availability requirements of the system. The function of the web application is only accessible to FAA-authorized personnel.

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 1370.121, FAA Information Security and Privacy Program and Policy which provides implementation guidance for the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the FISMA, Office of Management and Budget (OMB) mandates, NIST and other applicable DOT and FAA information and information technology management procedures. In addition to these practices, additional policies and procedures will be 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, and processing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness

DOT Privacy Office - Approved - 01/2020

training, as well as FAA Order 1370.121. The FAA will conduct periodic privacy compliance reviews of Privacy ICAO Address Program in accordance with the requirements of OMB Circular A-130.

Responsible Official

David E. Gray
Project Manager
David.E.Gray@faa.gov

Approving Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

DOT Privacy Office - Approved - 013020