U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration FAA

COA Application Processing System (CAPS)

Responsible Official

Eric Lautenschlager, Acting Manager, UAS Policy (AJV-P220)
Email: Eric.Lautenschlager@faa.gov
Phone Number: 202-267-3387

Reviewing Official

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

March 24, 2022

Executive Summary

The Federal Aviation Administration (FAA) Reauthorization Act of 2018, Pub. L. 115-254 Section 44807, *Special Rules for Certain Unmanned Aircraft Systems*, directs the FAA to integrate unmanned aircraft systems (UAS) safely into the National Airspace System (NAS). The FAA Air Traffic Organization (ATO) is responsible for implementing policies to integrate UAS operations into the NAS, while also collaborating with industry and across government. ATO has developed and implemented processes for granting operational approvals and waivers for UAS to fly in the NAS. The FAA issues a Certificate of Waiver or Authorization (COA) that permits persons, public agencies, organizations, and commercial entities to operate unmanned aircraft, for a particular purpose, in a particular area of the NAS as an exception to the FAA Regulations.

In support of this mission, ATO developed and implemented the COA Application Processing System (CAPS) to process the approval of Public[1] and Civil[2] COA applications submitted by both public and commercial proponents. A proponent (also known as an applicant or requestor) is the point of contact that represents the persons, public agencies, organizations, or the commercial entity responsible for submitting the information required to apply for a COA. CAPS is a web-based application that enables proponents to submit COA requests and allows FAA COA processors to efficiently and effectively assess and process COA applications.

This Privacy Impact Assessment (PIA) was developed pursuant to Section 208 of the E-Government Act of 2002 because the FAA is utilizing a web-based capability in which an applicant/proponent's personally identifiable information (PII) is collected to process their COA application.

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)

[1] Public Entity is defined to mean a Government of the United States; the District of Columbia, a territory or possession of the United States, or political subdivision thereof; any agency of the United States. Public entity examples include federal, state, and local government agencies that are recognized as political subdivisions of the State.

[2] Civil entity refers to ordinary citizens and their concerns, as distinct from military or ecclesiastical matters. Civil entity examples include companies, businesses and other organizations.

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.[3]

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 and System Overview

1.1 Introduction

The COA Application Processing System (CAPS) is a web-based application developed in support of the Federal Aviation Administration (FAA) Reauthorization Act of 2018, which directs the FAA to integrate unmanned aircraft systems (UAS) safely into the National Airspace System (NAS). A Certificate of Waiver or Authorization (COA) is an authorization issued by the Air Traffic Organization (ATO) to a civil or public operator for a specific unmanned aircraft (UA) activity. After the submission of a COA application, the FAA conducts a comprehensive operational and technical review. If necessary, provisions or limitations may be imposed as part of the approval to ensure the UA can operate safely with other airspace users. In most cases, the FAA provides a formal response within 60 business days from the time of submission. CAPS provides an interactive online application process to request a COA for a specific flight operation.

[3]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).

1.2 Background

Previously, the FAA relied on a manual, paper-based method to process Certificates of Waiver and Authorization (COA) applications. Proponents would request a COA to conduct operations or an activity using FAA Form 7711-2, *Application for Certificate of Waiver or Authorization*, which FAA used to determine whether to authorize public and civil entities to conduct operations that deviate from normal FAA Regulations. This information collection required physical verification (pilot certificates, aircraft inspections, etc.) by Aviation Safety Inspectors prior to approval. This manual process also involved coordinating with UAS pilots and Air Traffic Facilities to ensure the safe access to FAA NAS airspace for unmanned flights. To reduce the risks and burdens associated with a manual process for those operating within its critical infrastructure, the FAA introduced the UAS COA Online System. The UAS COA Online system was the first web-based application system, developed and implemented by the FAA that provided applicants with an electronic method of requesting a COA. In 2017, the system was decommissioned and replaced by CAPS. CAPS improved the preceding process by more efficiently automating the workflow associated with processing a COA. The gained efficiencies include, but are not limited to, the following:

- Utilizing a workflow and tasks model to automate the process of approving a COA application.
- Eliminating the need for COA Processors to send emails to record their comments and concerns. CAPS captures internal communication within the application.
- Providing map-layering services that allow applicants/proponents/requestors a standardized methodology for defining the area of operations, the obstacles, and boundaries in the desired UAS flight operation.
- Streamlining the approval process, creating a more user-friendly experience for the proponent and the FAA.
- Saving the agency money due to both the system, and its data, residing within the FAA.
- Saving resources by providing easy access to UAS monthly reports.

1.3 CAPS

CAPS is a web-based application that guides applicants/proponents and COA Processors through the various stages of the COA application process. CAPS utilizes a workflow model to automate the process of approving a COA application from its initial draft stage through its final stage. The workflow model provides detailed information on each stage of the COA application, review, and approval process to automate the FAA's ability to track each application's status, monitor progress, and take appropriate steps to ensure process deadlines

are met. It also defines who is responsible for and assigned to each step of the process. The workflow tracks the COA application as it progresses through the workflow and tracks data related to that application, such as who the application was assigned to and how long it has been in each stage of the application. Additionally, CAPS allows applicants/proponents to manage existing COA applications, start or cancel a new COA application, review the status of a previously submitted COA application, and submit reporting for a COA. The electronic process consists of four primary processes: Authentication and Access, Application, Review of Application, and COA Reports.

(i) Authentication and Access

CAPS is a web-based application that is accessible by applicants/proponents and COA Processors at https://caps.faa.gov. To access CAPS, users must first authenticate in MyAccess. External users authenticate using the FAA MyAccess External User Authentication Mechanism through a unique User ID, password, and challenge questions. After successful authentication, users are taken to the CAPS landing page where instructions in creating CAPS account can be obtained.

Once a proponent validates through the MyAccess electronic authentication process and is issued a FAA user account, the proponent can then request access to the CAPS online application program by completing the CAPS Access Request Form (see appendix A). The CAPS Access Request Form collects the Name, Public/Civil Entity, Telephone Number, Email Address, Area of Responsibility, and a description of the planned activities of the UAS. The proponent emails the CAPS Access Request Form to the CAPS mailbox at 9-AJV-115-UASOrganization@faa.gov for approval. CAPS Account Managers review the access request form. If approved, an account is created in CAPS and an email is sent to the proponent with access instructions. For public entities, a Public Declaration Letter (PDL)[4] may be required from the Agency's City, County or State Attorney's office. If a PDL is required, an account in CAPS is not created until the FAA's Legal Office (AGC-200) approves the PDL.

(ii) Application

Once access is granted, the proponent logs into CAPS using the FAA's External MyAccess authentication solution and completes the COA application.[5] The COA application collects

[4] The Public Declaration Letter (PDL) assures the FAA that the Proponent is recognized as a political subdivision of the government of the State under Title 49 of the United Stated Code (USC) section (§) 40102(a)(41)(C) or (D) and that the proponent will operate its Unmanned Aircraft in accordance with 49 USC. § 40102(a)(41)(C)(D) or (F) (not for commercial purposes "compensation or hire") and all public aircraft operations will meet the definition of a governmental function as defined in Title 49 USC 40125(a)2.
[5] COA operation types include a Jurisdictional COA that identifies a specific operating area and a Blanket Class G COA for operations within Class G contiguous United States.

the Name, Address, Email Address, and Phone Number from the applicant/proponent. CAPS automatically generates a unique numerical draft number used to track the application before its submission. Upon submission, CAPS then generates a unique COA Number[6] used to track the application throughout the COA process. Once the proponent enters their contact information, the proponent must acknowledge several statements called *Declarations*. The declarations section requires *Yes* or *No* responses from the proponent. Figure 1, *CAPS Declarations Section*, provides an example of the required statements. On this page, it is also required for the city, county, state, and tribal nation entities to upload their approved Public Declaration Letter (PDL). The document is uploaded into CAPS and does not contain any additional PII that was not previously captured during the application phase. The CAPS program does not allow the applicant/proponent to continue with the application until an approved PDL is uploaded.

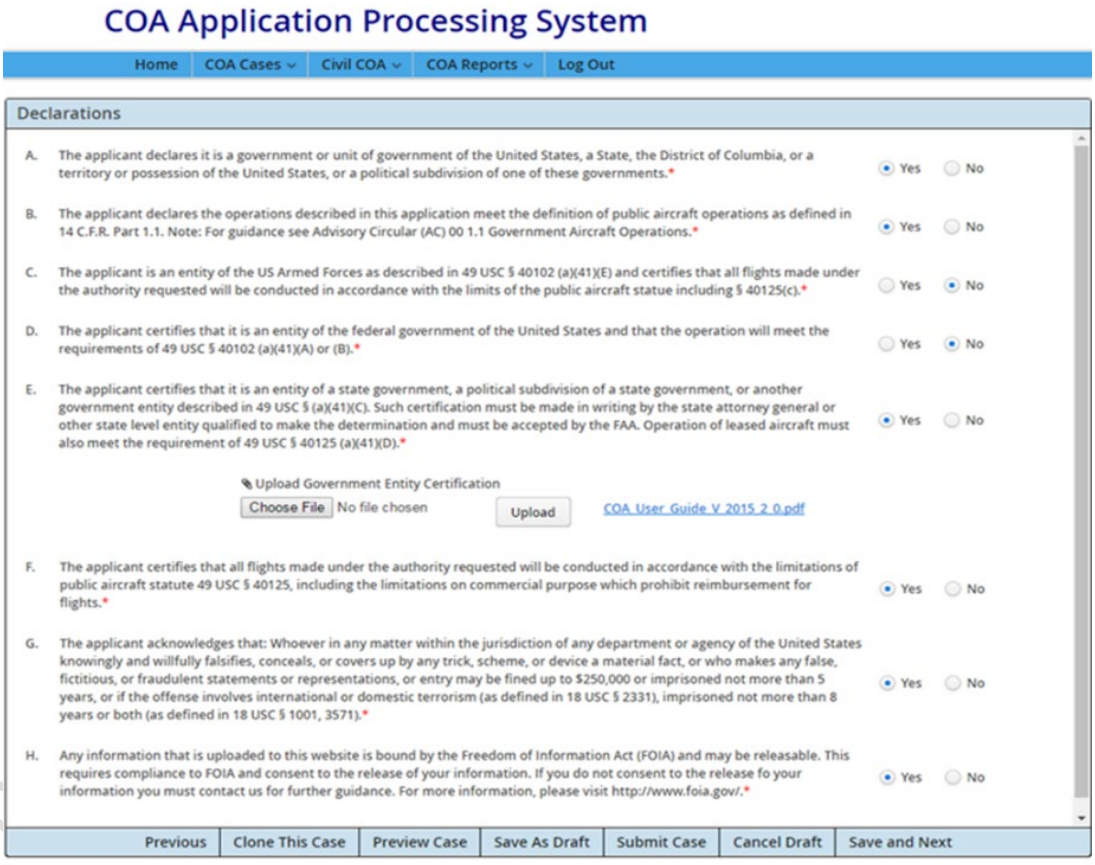

Figure 1 CAPS Declarations Section

[6] COA Numbers are comprised of the application year, 3-letter Service Area code, sequential number, and type of COA (e.g., 2021-ESA-1234-COA).

The COA application also collects information about the requested operation, flight operations area/plan, UAS specifications, and any flight crew qualifications. Some of the webform questions include free-form text fields; however, none of these fields specifically request or require additional PII from the proponent that is not outlined above. The COA Application also requires the proponent to include the following additional information:

- **Operational Description** — Overview of the proposed UAS activities to include the identification of the operating location (controlled and/or uncontrolled airspace), VFR/IFR operations, request for night and light out operations, and an executive and operational summary of planned UAS activities.
- **UAS Platform Specifications** — Information about the UAS platform to include performance characteristics, airworthiness certificate or declaration, lost link mission procedures, lost communication procedures, emergency procedures, aircraft lighting, spectrum analysis approval, ATC communications capability, electronic surveillance capability, and aircraft performance recording.
- **Visual Surveillance Methods and Procedures** — Description of the visual capability of the UAS operator to maintain visual contact with the UAS and a description of the resources to be utilized to maintain visual contact with the UAS and surrounding airspace.
- **Flight Operations Area/Plan** — The geographic location of the requested operation.
- **Flight Aircrew Qualifications**[7] — Series of *Yes* or *No* radio buttons and free text fields to identify any relevant information regarding the training or certification of the aircrew, medical certification, and duty time restrictions.
- **Special Circumstances Description** — Amplifying information that may help determine the feasibility of the operation.

[7] Flight Aircrew Qualifications include FAA or DOD Equivalent Type of Pilot or Observers, Training (DOD Certified/Trained, Other Certified Training, and Training on FAR Part 91) Medical Certification Class, including Currency Status and Duty Time Restrictions. This information is anonymous and is not linked to any individual.

(iii) Review of Application

Figure 2, *CAPS Informational Flow*, illustrates the COA application process. When a proponent submits a COA application, CAPS automatically sends an email notification to the appropriate COA Processor informing them of the proponent's submission. The COA Processor logs into CAPS using MyAccess authentication. The COA Processor then reviews the application for completeness and ensures that all required attachments are included. The COA Processor works with the proponent to clarify or correct inconsistencies in the application. The COA Processor can return the application to the proponent for further refinement or begin the workflow process to submit it to the next reviewer (Air Traffic Control Specialists or Aviation Safety Inspector). This review process is repeated until all necessary parties (reviewer groups) have approved the application or it is determined that it cannot be approved[8]. Once the COA is granted and the COA becomes active, a signed .pdf copy of the COA is sent to the proponent. If disapproved, the COA processor sends a disapproval letter stating the reason for the disapproval. Once the application is complete, the COA application and all relevant documentation are stored in CAPS.

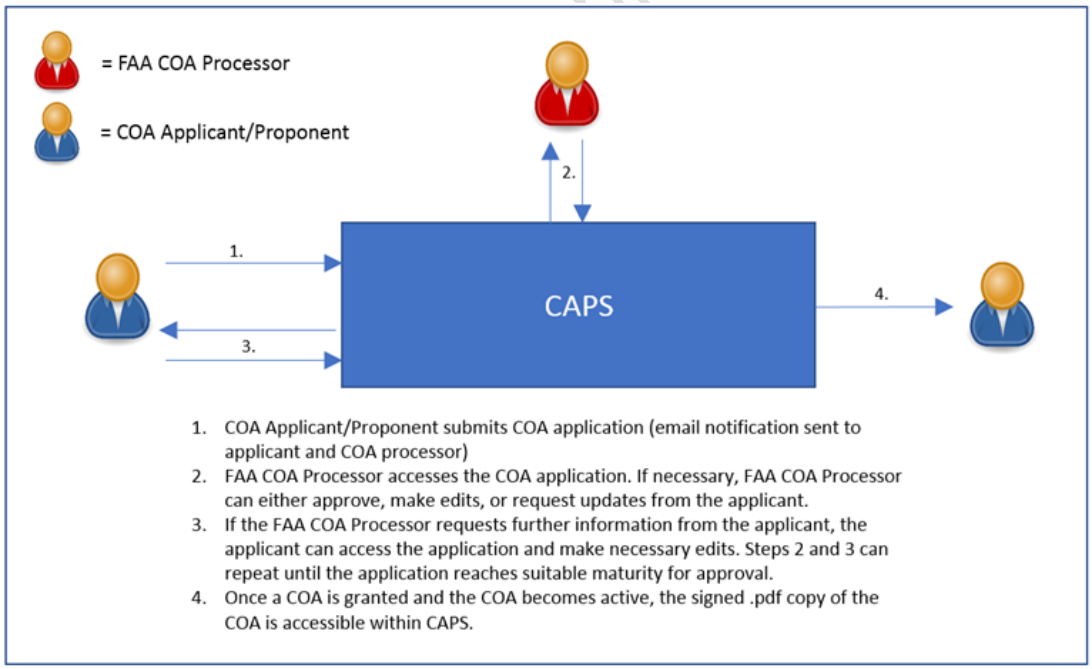

Figure 2 CAPS Informational Flow

[8] A reason for a COA denial is the facility could not support the proponent's operations due to the location reference arrival and departure flight path or the proponent did not provide sufficient mitigations to safely perform the requested operation.

(iv) COA Reports

As specified under the Special Provisions of the COA, proponents must comply with certain reporting requirements. The requirements, as listed under Section D, *Reporting Requirements*, are:

(1) Documentation of all operations associated with UAS activities is required regardless of the airspace in which the UAS operates.
(2) The Proponent must submit the number of flights monthly through the COA Application Processing System (CAPS).

In support of this requirement, the intake and storing of reporting data was developed and implemented in CAPS. Proponents submit their monthly UAS reports by selecting the *Create Report for Public/Civil COA* link from the Home page. On the COA Reports page, the proponent clicks on the *Submit Monthly Report* button to commence reporting. The COA report application requests the proponent's name and contact information. It also collects information about the aircraft, operating hours, flight information (e.g., Flight Date, Aircraft Operational Hours, GCS Operational Hours, Pilot Duty Time per PIC, Location City/Name, Latitude, Longitude, and Number of Flights at Location). Additionally, the COA report application requests lost communication events, equipment malfunctions, lost link events, deviations, take-off/landing damage, and a description of any other operational/coordination issues, which occurred during the month. Once the report is complete, the proponent submits it to the FAA. Some of the web form questions include free-form text fields; however, none of these fields specifically request or require additional PII from the proponent. No decisions about individuals or individual applications are made based on these reports—the approval/denial of a COA application is based solely on the merits of the application. Additionally, no new data is generated through the CAPS reporting methods.

1.4 System Users

System users are categorized as *external* users or *internal* users, where external users are proponents, applicants, or requestors and internal users are comprised solely of FAA personnel.

(1) External Users

- External users include public and civil entities.
- A proponent is the point of contact that represents public agencies, organizations, or a commercial entity submitting a COA application.

- External users authenticate using the FAA MyAccess External User Authentication Mechanism[9] through a unique User ID, password, and challenge questions.
- Once authenticated to the FAA network, the proponent accesses the site through a client browser on a public website at https://caps.faa.gov.
- External users never directly access internal FAA AIT infrastructure.
- PII collected and used in the CAPS system for external users includes:
  - Name,
  - Address,
  - Phone Number, and
  - E-mail Address.
- No Social Security Numbers are collected or used.
- Users are asked, using *Yes* or *No* radio buttons, if the COA operator has a pilot's license, and the class of medical certificates.
- No health-related information is collected or used.
- No financial information is collected or used.
- Since the external users' access to the CAPS program is limited to only being able to view information entered by the external user through their email log-in account, external users cannot view other account users' applications.

(2) Internal Users

- Internal users are comprised of FAA personnel who are responsible for assessing and approving COAs.
- CAPS internal FAA users access the system via a client browser, such as Google Chrome, and access CAPS using their Personal Identity Verification (PIV) card via the FAA MyAccess authentication solution.
- Upon successful FAA MyAccess authentication, CAPS will receive the user's username, reference the authorization controls in the CAPS database, and then assign appropriate permissions.
- PII collected and used in the system for internal users includes:
  - Name,
  - Username, and

[9] If the proponent is not an FAA internal user, they must register for an FAA account using the FAA MyAccess electronic authentication process, which uses an authorized third-party identity proofing service (IdSP) to verify the individual is who they claim to be. If the individual successfully completes the identity proofing process, the FAA receives a response from the IdSP containing the result of the authentication; however, the FAA does not receive nor store the individual's information submitted for identity-proofing purposes. When FAA receives the IdSP response, FAA creates a user account for access (unique MyAccess ID). For more information regarding MyAccess privacy practices, please see the FAA MyAccess/Electronic Identity Authentication Service Privacy Impact Assessment located on the DOT Privacy website.

- Email Address.

CAPS has the following FAA Reviewer groups that provide review and oversight of the application:

FAA Primary Reviewer (COA Processors):[10]	Serves as point of contact for the applicant/proponent during the COA application process. Conducts the initial and final review of the application to include the approval or denial of the COA; oversees the COA application through the review process, addressing any concerns from the facility that has jurisdictional responsibility for the proposed operating area. They are the focal point for the coordination between the applicant/proponent and other agencies. Feedback is through email, phone call, or in the comments section of the COA application.
FAA Management:	Serves as the designated signatory authority for the approval or denial of the COA Application.
FAA Aviation Safety Inspector:	Conducts a safety review of the COA application; provides feedback to the applicant/proponent through the FAA Primary Reviewer.
FAA Safety Management:	Approves or denies the safety review on behalf of the FAA Safety Office; designates and coordinates with the FAA Safety Inspector and the FAA Primary Reviewer.
FAA Gatekeeper (Account Manager):	Has general oversight of all COA applications, assists with account management; provides approval or denies access to CAPS and system issues.

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, is 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 risks. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families

[10] The FAA Primary Reviewer is at the service center level.

articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[11], 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[12].

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 takes steps to ensure transparency and that applicants/proponents are aware of the procedures for submitting a COA application and the purposes for which the FAA collects and maintains personally identifiable information (PII) in support of CAPS.

FAA uses multiple communication methods to promote applicant awareness of the procedures for submitting a COA application and the purposes for which the agency collects and maintains PII in support of CAPS. Communication methods include but are not limited to websites, emails, phone calls, and online meeting forums.

FAA holds public forums, webinars, and an annual FAA UAS Symposium where information is provided on authorizations, waivers, and relevant processes. Along with this public outreach, the FAA's Unmanned Aircraft System (UAS) website (https://www.faa.gov/uas/) is the central point for UAS stakeholders to collect UAS information and includes frequently asked questions that speak to UAS requirements, policies, and regulations. The FAA makes public and adheres to FAA Order 7200.23, *Processing of Unmanned Aircraft Systems Requests* and FAA Order 7210.3, *Facility Operation and Administration*, which provide policy and guidelines for the approval or denial of a COA.

CAPS retrieve records by an individual's name and other personal identifiers. The FAA processes Privacy Act records by the following published system of records notices (SORN):

[11] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[12] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

- DOT/FAA 854 - Small Unmanned Aircraft Systems (sUAS) Waivers and Authorizations, 84 FR 32512 (July 8, 2019). SORN DOT/FAA 854 currently provides notice to the public of FAA's privacy practices regarding the collection, use, sharing, safeguarding, maintenance and disposal of information collected from Part 107 operators related to waivers and authorizations.
- DOT/ALL 13, *Internet/Intranet Activity and Access Records* (67 FR 30757). This SORN covers the collection and maintenance of Names and Email Addresses of FAA employee users.

As required, a Privacy Act Statement discussing the Department's privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information is included on the CAPS home page.

Lastly, the FAA's publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the CAPS Program.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

CAPS uses data collected directly from the individual for the processing of COA applications. Under the provisions of the Privacy Act, individuals may request searches to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, S.W.
Washington, DC 20591

The following information must be included in the request:

Name
Mailing address
Phone number and/or email address
A description of the records sought, and if possible, the location of the records

Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for why the records should be corrected, to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, S.W.
Washington, DC 20591

If the applicant/proponent determines that the source information for the COA is inaccurate, the applicant/proponent may submit a correction request. The FAA will then determine the accuracy of the information and if a correction to the data is, appropriate. If required, the necessary correction will be made to the record in CAPS.

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.

The FAA is required to collect and maintain information about applicants/proponents and UAS operations in support of the Federal Aviation Administration (FAA) Reauthorization Act of 2018, Pub. L. 115-254 Section 44807, *Special Rules for Certain Unmanned Aircraft Systems*, which directs the FAA to integrate UAS safely into the NAS. CAPS collects and processes PII from applicants/proponents for the following purposes:

1) System Access: Person's name, email, and phone number.
2) Point of Contact Information on COA Application: Name, email, physical address, and phone number (business or personal)

The FAA also uses this system to support FAA safety programs and agency management, including safety studies and assessments by the FAA's Privacy Act System of Records Notice DOT/FAA 854 - Small Unmanned Aircraft Systems (sUAS) Waivers and Authorizations, 84 FR 32512 (July 8, 2019). The FAA may use the point of contact information provided with requests for waivers or authorizations to communicate and provide information about potentially unsafe conditions to UAS owners and operators and to educate them regarding safety requirements for operation. The FAA uses this system to maintain oversight of FAA-issued waivers or authorizations, and records from this system may be used by FAA for enforcement 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.

FAA devoted significant effort to designing the CAPS application to help ensure the FAA collects the minimum amount of information necessary to establish and maintain a record to issue a COA. CAPS collects and retains the following information from proponents: Name, Address, Email Address, and Phone Number. The name and email address are used to process the CAPS application, while the remaining information is used to contact the proponent, as necessary. CAPS generates a unique number used to track the application before its submission, and a unique COA Number[13] that tracks the application after its submission. The FAA COA Processors use the Name and Email Address to contact the COA proponent to ensure application accuracy, verify information, or gain other pertinent information required to process the COA. CAPS data includes forms that are uploaded by the proponent. None of these forms specifically request or require additional PII.

The COA data retention policy is described in the Record Retention Schedule No. DAA-0237-2016-0019. The Record Retention Schedule imposes that authorization or waiver data will be disposed of after three years following the expiration of the waiver or authorization. The Record Retention Schedule includes additional retention policies for cases in which the request is not authorized.

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.

FAA takes steps to ensure that the information in CAPS is used only for the purposes for which it was collected. CAPS guidance material and training are provided to stakeholders, the public, the COA Processors, ATC facilities, and other interested parties. CAPS guidance material may consist of user manuals, emails, and other distributable information. Training for CAPS is provided via online meeting forums such as Teams and Zoom.

In addition, the processing of CAPS information is covered by the Department's system of records notice DOT/FAA 854 - Small Unmanned Aircraft Systems (sUAS) Waivers and Authorizations, 84 FR 32512 (July 8, 2019). In addition to other disclosures generally permitted under 5 U.S.C. § 552a (b) of the Privacy Act, all or a portion of the records or

[13] COA Numbers are comprised of the application year, 3-letter Service Area code, sequential number, and type of COA (e.g., 2021-ESA-1234-COA).

information contained in this system may be disclosed outside DOT as a routine use according to 5 U.S.C. § 552a (b) (3) as follows:

1. To the public, including aircraft operator/owner's name, affiliated organization (if any), mailing address, remote pilot's name, certificate number, small UAS type, small UAS registration number, waiver beginning, and end date and time, location of operations, class of airspace, altitude, description of the proposed operation, and any history of previous, pending, existing, or denied requests for waivers and authorizations applicable to the small UAS at issue for purposes of the waiver, and special provisions applicable to the small UAS operation that is the subject of the request. The FAA will also disclose to the public waiver denials, which may include the aircraft operator/owner's name, affiliated organization (if any), mailing address, remote pilot's name, certificate number, small UAS type, small UAS registration number, and rationale for the denial. Email addresses and telephone numbers will not be disclosed under this Routine Use. Airspace authorizations the FAA issues under 14 CFR § 107.41 will not be disclosed under this Routine Use, but the FAA will disclose the actual waiver that waives the applicability of § 107.41.[14]

2. To law enforcement, when necessary and relevant to an FAA enforcement activity.

The Department has also published 14 additional routine uses applicable to all DOT Privacy Act systems of records. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, and 77 FR 42796, July 20, 2012, under ''Prefatory Statement of General Routine Uses.''[15]

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

The following processes are in place to ensure the quality and integrity of information within CAPS:

First, CAPS information is collected directly from the individual (called a "proponent") submitting the COA application. The proponent is responsible for the accuracy of the information they provide when submitting a COA application. Additionally, once a COA application is submitted, the COA Processor reviews the application information for

[14] https://www.transportation.gov/individuals/privacy/privacy-act-system-records-notices
[15] https://www.gpo.gov/fdsys/pkg/FR-2016-08-02/pdf/2016-18208.pdf

completeness and ensures that all required attachments are included. The COA Processor works with the proponent to clarify or correct inconsistencies in the application. The COA Processor can return the application to the proponent for further refinement or advance it to the next reviewer (Air Traffic Control Specialists or Flight Safety Specialists) in the COA process. The review process is repeated until all necessary parties have approved the application or it is determined that it cannot be approved,[16] at which point, the COA is granted or a denial letter is issued.

CAPS also leverages the following additional controls to promote data quality and integrity:

- CAPS provides role-based separation of duties and limited access to reduce the risk of unauthorized changes/edits to the data. System rights are explicitly assigned such that individuals can only access those functions necessary for the job functions such individuals perform as users of the system.
- Additionally, the system does not allow account sharing of any kind to limit the exposure of data to unauthorized third parties.
- CAPS does not receive or transmit any application data to any other system.
- CAPS guidance material and training are provided to stakeholders, the public, the COA Processors, ATC facilities, and other interested parties. CAPS guidance material may consist of user manuals, emails, and other distributable information. Training for CAPS is provided via online meeting forums (e.g., Teams, Zoom).

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.

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. Additionally, CAPS incorporates standards and practices for federal information systems as directed under the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security*

[16] A reason for a COA denial is the facility could not support the proponent's operations due to the location reference arrival and departure flight path or the proponent did not provide sufficient mitigations to safely perform the requested operation.

and Privacy Controls for Federal Information Systems and Organizations, dated September 2020.

CAPS is a General Support System and is deployed within an FAA maintained/operated production environment located at the Mike Monroney Aeronautical Center (MMAC) in Oklahoma City, Oklahoma. The MMAC is responsible for providing physical access control to the campus and maintains the physical access control for the buildings and select rooms, including the Enterprise Data Center (EDC).

CAPS routinely undergo a security review process under the FAA NAS Security Office. This process ensures the CAPS application and program meet the necessary security standards and controls to operate in a production operation.

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, *Information Security and Privacy Program & Policy*. FAA Order 1370.121 implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the Federal Information Security Management Act (FISMA), Department of Transportation (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 personally identifiable information. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of the CAPS web application relative to the requirements of OMB Circular A-130.

Responsible Official

Eric Lautenschlager
System Owner
Acting Manager, ATO – AJV-P220

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

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

Appendix A: CAPS Access Request Form

Certificate of Operation (COA) Application Processing System (CAPS) Access Request Form

The Certificate of Waiver or Authorization (COA) Application Processing System (CAPS) is a web application developed in support of the Federal Aviation Administration (FAA) Modernization and Reform Act of 2012 (FMRA), PL 112-95, § 333 & 334. The FMRA directs the FAA to safely integrate Unmanned Aircraft Systems (UASs) into the National Airspace System (NAS). CAPS provides an interactive on-line application process to request a COA for a specific flight operation, or a blanket COA, which permits nationwide flights under standard restrictions.

In order to gain access to CAPS and complete a COA, please complete this form and submit in accordance with the instructions provided at https://caps.faa.gov.

If you are not sure about which type of waiver or authorization is needed for your UAS operation, please visit www.faa.gov/uas.

Section 1: Proponent Information

Date	Name
Public/Civil Entity	
Telephone	Email

Is requester a contractor for a public entity? ◯ Yes ◉ No If Yes, proceed to Section 2. If No, proceed to Section 3.

Section 2: Contractor Requests

Contractors must submit this form along with a signed letter from the authorizing agency for public requests.

Example #1: This letter is to authorize (Contractor Name), of (Company Name), (Company Address), on-line access to the (Public/Civil Entity) COA documents and process.

Example #2: This letter is to authorize (Contractor Name), of (Company Name), (Company Address), on-line access to the (Public/Civil Entity) COA documents, process, and to serve as the primary point of contact in all COA matters.

Section 3: Permissions

☐ I am requesting the ability to draft, update, and commit COAs on behalf of the (Public/Civil Entity) listed above. I will be applying for the following COA type (select all that apply): ☐ Civil ☐ Public - non DOD ☐ DOD

Section 4: UAS Operation(s)

Area of Responsibility (AOR) Please indicate the county and state where the UAS will operate.	
Provide us with a reason why you are using a UAS. **Example #1**: I will submit COA applications for the (Name of University) which is developing a UAS program to address law enforcement and emergencyresponseapplications. **Example #2**: I am a UAS operator and the UAS Tier 1 Projects Officer for Marine Corps Systems Command and will be conducting flight demonstrations for VIP visitors. (SES and Flag officers). I will need to establish an account in order to create COA requests. **Example #3**: I will submit COA applications for the (Name of University) which is developing a UAS program for the purpose of research and development. Initially research efforts will focus on agricultural applications but eventually will move into other areas of UAS technology development and applications. **Example #4**: I just started working UAS Airspace issues for the Air Force Special Operations Command. I will need to establish an account in order to create COA requests.	

PRIVACY ACT STATEMENT: This statement is provided pursuant to the Privacy Act of 1974, 5 USC § 552a.The authority for collecting personally identifiable information (PII) through the COA Application Processing System (CAPS) website is contained in 14 CFR Part 107 which permit small UAS operators to apply for certificates of waiver to allow a small UAS operator to deviate from certain provisions of 14 CFR part 107 if the Administrator finds the operator can conduct safely the proposed operation under the terms of a certificate of waiver. In addition, it permits operators to request authorizations to enter controlled airspace (Class B, Class C, or Class D airspace, as well as the lateral boundaries of the surface area of Class E airspace designated for an airport). The principal purpose for which information collected is intended to be used is to complete the COA process and receive a response. Failure to provide the required information will prevent the FAA from granting a certificate of waiver or authorization which is required by 14 CFR part 107 to be completed prior to operation of the small UAS. The information collected to complete the COA process and issue the unique identifier is included in a Privacy Act System of Records known as DOT/FAA 854, titled "Requests for Waivers and Authorizations Under 14 CFR Part 107 – 81 FR 50789 – August 2, 2016." Records from this system of records may be disclosed in accordance with the routine uses that appear in Department of Transportation (DOT)/FAA 854, available at https://www.transportation.gov/individuals/privacy/privacy-act-system-records-notices.