



U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Air Traffic Organization (ATO)

**Drone Information for Safety, Compliance, Verification,
and Reporting**

(DISCVR)

Responsible Official

Mike Torrence

Email: Mike.Torrence@faa.gov

Phone Number: (609) 485-5263

Reviewing Official

Karyn Gorman

Chief Privacy Officer

Office of the Chief Information Officer

privacy@dot.gov





Executive Summary

The Federal Aviation Administration (FAA) Air Traffic Organization (ATO) operates the Drone Information for Safety, Compliance, Verification, and Reporting (DISCVR) system under authority [49 U.S. Code § 40101](#). The DISCVR system is a tool designed to support select personnel within the FAA, the Department of Defense (DoD), and the Department of Homeland Security (DHS) with accessing and managing data related to drone operations. DISCVR enhances the ability to process airspace authorizations and ensure compliance with aviation regulations by providing a secure interface to search and sort data from the FAA Drone Zone (DZ) registration databases and the Low Altitude Authorization and Notification Capability (LAANC). DISCVR also provides real-time data access to FAA air traffic security specialists for waiver and authorization data.

The FAA is publishing this Privacy Impact Assessment (PIA) for DISCVR in accordance with Section 208 of the [E-Government Act of 2002](#) (Public Law 107-347). Although the system itself does not store data, it can access Personally Identifiable Information (PII) from members of the public. This includes data from small Unmanned Air System (sUAS) registrants sourced by FAA DZ and LAANC. DISCVR acts as an interface for querying and sorting existing data while ensuring robust privacy and security protocols are maintained.

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 DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

¹Office 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).



- *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 PLA, 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 DISCVR system assists select personnel within the FAA, DoD, and DHS in accessing and organizing data related to drone operations for authorized purposes of enhancing public safety, preserving the integrity of U.S. airspace, and supporting national security. In pursuing these goals, authorized DISCVR users can utilize the tool to identify and contact the operator of a sUAS flying in an unsafe manner that endangers public safety. DISCVR serves the following user groups:

1. **FAA Law Enforcement Assistance Program (LEAP) Agents and Aviation Safety Inspector (ASIs):** These individuals are responsible for enforcing compliance and maintaining safety standards within aviation operations.
2. **DoD Authorized Users:** Personnel from the DoD who require access to drone operation data for national security and defense purposes.
3. **DHS OCIO Geospatial Information Infrastructure (GII) System Users:** As an external partner, the DHS GII system facilitates geospatial data sharing and collaboration, enhancing situational awareness and operational coordination.

Key Functions and Capabilities:

- **Search and Sort:** DISCVR enables users to search through data fields in the FAA DZ registration databases and LAANC. This functionality ensures efficient retrieval of information related to airspace authorizations and waivers.
- **Real-time Data Access:** The system provides real-time access to information from sUAS operators, which is essential for processing requests to operate drones in specific classes of airspace, including Class B, C, D, and certain Class E areas around airports.



- **Privacy and Security:** While DISCVR itself does not store any data, it serves as an interface for querying and sorting existing data in the FAA DZ and LAANC databases. Both databases adhere to strict privacy and security protocols.
- **PII Querying Capability:** Although DISCVR does not maintain or collect PII for its operations, it can access and display PII from the FAA DZ as needed. This includes details such as the registrant's name, contact information, and specifics about the drone, like its make, model, and remote ID serial number. This information is vital for identifying the owners of sUAS operating in an unsafe manner (i.e. conducting unauthorized operations in Class B, C, or D airspace, flying in restricted airspace, or operating above the max altitude threshold set for sUAS).

In summary, DISCVR enhances the ability of the FAA, DoD, and DHS's ability to manage and monitor drone operations, ensuring compliance with airspace regulations while maintaining privacy and security measures.

User Access

Internal User Access

FAA user access to DISCVR is provided through MyAccess (Personal Identity Verification [PIV] credentials), centralized identity access management (CIAM)² by permitting specific FAA Lines of Business, such as ASH ss Agents (AXE) and AVS ASI access to the DISCVR production environment. Within the FAA, a user with valid credentials accesses the DISCVR website (<https://discvr.faa.gov/DISCVR/#/>). The DISCVR API is central to the platform, permitting access to FAA users and external inter-agency partners.

External User Access

The DISCVR API permits sharing FAA DZ and LAANC data with external federal partners and security agencies using access tokens.

External users have accounts with their own federal entity (i.e. not FAA MyAccess). That external federal entity is responsible for developing a User Interface (UI) environment for their own authorized users, which accesses the DISCVR API. DISCVR only maintains PII from external users such as username.

DHS developed their own UI environments for DISCVR access and manages user authentication internally. The FAA and DHS have a signed Memorandum of Agreement (MOA) and Information Security Agreement (ISA) between organizations. The MOA sets forth the mutual understanding of data access and handling to ensure that the FAA PII and

² The FAA's CIAM is delivered through its MyAccess platform, which provides a single sign-on and identity authentication service for public citizens and non-FAA users accessing DOT/FAA systems, using a third-party identity service provider (IdSP) and integrated with Login.gov.



small sUAS data, collectively “UAS data”, exchanged between the parties pursuant to this MOA is managed in accordance with FAA and DHS regulations and policies to protect any PII.

DoD developed a pilot UI environment for DISCVR and manages user authentication internally. The ISA between DoD and FAA was signed in March 2026. The MOA between the FAA and DoD has not yet been signed by all parties; however, the FAA has approved and signed a Temporary Access to DISCVR action memo granting DoD temporary permission to DISCVR while the MOA is finalized.

These agreements ensure that all parties adhere to the necessary security and privacy standards.

Typical Transactions

A typical transaction begins with an FAA employee receiving a request from a law enforcement, DoD, or DHS partner to obtain contact information about a sUAS operator who was reportedly flying a drone in an unsafe manner or posing a risk to national security. In one example, an sUAS operator flew their sUAS over a college stadium during a football game with over 30,000 attendees. Using a wireless device capable of receiving a Remote Identification (RID) module broadcasting Radio Frequency (RF) signals, the local law enforcement agency was able to obtain the Serial Number from the sUAS. The serial number is a unique identifier of the sUAS included in the broadcast signal. It is attributed to the sUAS through the FAA DZ registration process by the person responsible for the sUAS.

In the typical transactions scenario, the serial number obtained by law enforcement is used to query the sUAS Operator Registration information via the internal DISCVR UI (alternatively, the query can be conducted by an FAA employee if the external partner does not have an active MOA and ISA). This returns the sUAS registration number which is then used to query information regarding the sUAS operator by retrieving FAA DZ and LAANC Airspace Authorization data. This query displays information associated with the initiated search within the UI associated with user.

Information displayed by DISCVR UI or external partner UI may contain PII of a sUAS owner, operator, or commercial company in the contact information context needed for further coordination with Air Traffic Control (ATC) or contact with investigating authorities.

The DISCVR query response window may or may not include sUAS or RID module serial number, make and model, owner and operator name, organization, telephone number, address,



email address, etc., depending on the completeness of the information provided to DZ and LAANC.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.

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.

DISCVR does not collect PII. The FAA deploys a variety of means to ensure that individuals are informed about the collection, use, and safeguarding of their PII as it pertains to DISCVR. For example, the FAA provides notice of the collection of PII that may be viewable via DISCVR through the following UIs:

Declaration of Compliance: Collects the registrant's name, mailing address and email address.

Means of Compliance: Collects the registering individual or organization's name, mailing address, telephone number, and email address.

Notice of Identification: Collects the registrant's name, mailing address, email address, and phone number.

Further, the FAA promotes transparency of DISCVR by publishing appropriate privacy compliance documentation. This PIA is published in accordance with E-Government Act of 2002, to ensure public awareness of the information handling practices associated with the DISCVR system. In addition, to further transparency, DOT has published the following System of Records Notices (SORNs), which are related to this system:



[DOT/FAA 854 – Small Unmanned Aircraft Systems \(sUAS\) Waivers and Authorizations, 88 FR 59566 \(August 29, 2023\)](#), which pertains to records within FAA DZ and LAANC on individuals operating sUAS who request and receive authorizations to fly in controlled airspace or waivers to fly outside of the requirements of the Code of Federal Regulations (CFR) and to review and approve Certificate of Waiver or Authorizations (COA) applications. Information covered includes; operator information: name, address, and email; and unmanned aircraft information such as manufacturer name, model name, serial number, longitude/latitude/geometry, country of registration, and registration number. This information is viewable in DISCVR but is not collected or maintained therein.

[DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 \(May 7, 2002\)](#), which applies to information collected and maintained in support of FAA systems, which covers system access records maintained in DISCVR.

As previously stated, DISCVR does not collect or maintain PII, but provides a secure interface to search and sort data from the FAA DZ registration databases and LAANC. Individuals seeking redress through the source systems should reference the [FAA DZ PIA](#) or [LAANC PIA](#) for instructions.

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.

PII queried from DZ may be present in the *Notice of Identification* submitted by the individual who wishes to operate a foreign-registered civil unmanned aircraft in the United States.

Under the Privacy Act, individuals may request a search to determine whether any records have been added that may pertain to them. Individuals wishing to know if their access records under DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002) appear in a system may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington, DC 20591

Included in the request must be the following:



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

Contesting Record Procedures

Individuals who believe information relating to system access for DISCVR is inaccurate or incomplete may request corrections. These requests should be submitted in writing with an explanation of the correction sought to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

DISCVR queries FAA DZ and LAANC to view information about sUAS operators and to receive and respond to requests for authorization to operate a sUAS in Class B, C, or D airspace, or within the lateral boundaries of the surface area of Class E airspace designated for an airport.

Information collected by the UAS Service Suppliers (USS) is maintained in accordance with its own privacy policy. The MOA between the USS and FAA, and its associated Performance Rules, contains requirements for the USS to have a privacy policy in place and to provide a privacy statement to users. If a violation of the MOA or its Performance Rules occurs, the FAA can revoke the USS's MOA.

The FAA collects and uses PII associated with sUAS (the registrant's name, organization, telephone number, mailing address, email address.), and other information (aircraft manufacturer name, model name, serial number, and country of registration) for the authorized purposes of enhancing public safety preserving the integrity of U.S. airspace and supporting national security. The FAA may use the sUAS operator's contact information to provide information about potential unsafe conditions to sUAS owners and operators and to educate those regarding possible risks to their operation.



Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

The FAA collects and stores information within LAANC from persons who operate foreign-registered civil unmanned aircraft in the United States to support the identification of those aircraft when operating within U.S. airspace. The FAA collects only the minimum information necessary to link a declaration of compliance to the applicant who submitted it and the sUAS to which it applies. The FAA likewise collects the minimum amount of information from applicants who submit a means of compliance to ensure continued compliance with the rule's performance-based requirements.

The FAA maintains records in accordance with the following National Archives and Record Administration (NARA) approved General Retention Schedules (GRS):

- Copies of electronic records that are not deemed official agency records are covered under [GRS 5.1: Common Office Records, item 20](#). These records are temporary and are destroyed immediately after copying into a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.
- System access records are covered under [GRS 3.2, Information Systems Security Records, item 030](#). These records are temporary and are destroyed when business use ceases.
- System access records that require special accountability for access are covered under [GRS 3.2, Information Systems Security Records, item 031](#). These records are destroyed 6 years after the password is altered or user account is terminated.

Two important exclusions apply: these records do not cover electronic signature data, nor do they involve monitoring for agency mission-specific activities such as law enforcement operations.

Non-record copies and access records are retained only as long as they are actively used for business purposes. Once that use ends, they are destroyed in accordance with the approved retention schedule.

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.



As noted above, there is no collection of PII by DISCVR. DISCVR is only a search-and-sorting tool for the DZ and LAANC databases. The use of PII related to sUAS registrants, including contact information, aircraft manufacturer name, model name, and serial number, and country of registration, serves the authorized purpose of enhancing public safety, maintaining the integrity of U.S. airspace and supporting national security efforts. The data is not used for any other purposes. The serial number data element is broadcast by sUAS operators during flight and, when necessary, are correlated with FAA registry records to identify aircraft and contact registered operators in connection with safety incidents or violations.

A signed MOA and ISA are necessary before DISCVR access token distribution to DoD, DHS, and federal law enforcement partners. When PII is shared with external partners (law enforcement agencies, national security entities, other oversight bodies engaged in aviation-related investigations or enforcement), such sharing is limited to the minimum necessary for the intended purpose. All FAA personnel with access to PII receive role-based privacy and security training and are subject to DOT and FAA policies governing the appropriate use of data.

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).

DISCVR enforces required fields and role-based access, helping maintain accuracy and completeness. Any outdated or inaccurate PII is corrected, as necessary, during routine reviews.

These measures help ensure that decisions regarding the operation and oversight of DISCVR are based on reliable, up-to-date information, thereby supporting both safety and regulatory compliance in the National Airspace System (NAS).

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 Publication 200, Minimum Security Requirements for Federal



Information and Information Systems, dated March 2006, and the NIST and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 2020.

DISCVR implements robust security controls, including role-based access and secure tokens. All access is subject to logging and monitoring. In addition, FAA employees working with the system are required to complete both privacy and IT security training annually. These training requirements are enforced across all FAA programs handling sensitive information.

If these credentials are not tied to their MyAccess identity, they will be denied permission to DISCVR. It's a "deny all" approach in which DISCVR allows only specific users. DISCVR worked with the CIAM team to enable this tagging methodology. As FAA employees leave the agency, change roles, or do not log in within 90 days, MyAccess automatically removes those permissions. No actions are required by the owners of DISCVR or AIT. New employees in applicable lines of business receive credentials tied to their PIV card.

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.

The FAA's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division is responsible for governance and administration of FAA Order 1370.121B, FAA Information Security and Privacy Program Policy. FAA Order 1370.121B implements the various privacy requirements based on the Privacy Act, the E-Government Act of 2002 (Public Law 107-347), the FISMA, DOT privacy regulations and policy, OMB mandates, and other applicable procedures and guidance.

In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to the protection, retention, and destruction of records. Federal and contract employees who work with DISCVR receive clear guidance on their duties related to collecting, using, processing, and securing privacy data. Guidance is provided through mandatory annual security and privacy awareness training and the FAA Privacy Rules of Behavior. The FAA periodically conducts privacy compliance reviews of all FAA systems that retain and/or process PII in accordance with the requirements of the OMB Circular A-130.



Responsible Official

Mike Torrence
System Owner
Manager, Aeronautical Data Systems
AJM-337

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN
MARIE
GORMAN

Digitally signed by KARYN
MARIE GORMAN
Date: 2026.09.21 15:17:48
-04'00'

DOT Privacy Office - Approved - 09/21/2026