



U.S. Department of Transportation

**Privacy Impact Assessment  
Federal Aviation Administration (FAA)  
Office of the Chief Counsel (AGC)  
Case and Document Management System  
(CDMS)**

**Responsible Official**

Tracy Cotton  
Managing Director  
Office of the Chief Counsel  
(202) 267-3222

**Reviewing Official**

Karyn Gorman  
Chief Privacy Officer  
Office of the Chief Information Officer  
[privacy@dot.gov](mailto:privacy@dot.gov)





## Executive Summary

The Federal Aviation Administration (FAA) Office of the Chief Counsel (AGC) provides legal services to the FAA. These services include offering legal advice, reviewing agency actions for compliance with legal requirements, representing the FAA in a variety of legal matters, and conducting administrative adjudications in-house. Specifically, AGC70 and AGC 600 conduct in-house administrative adjudications under 14 CFR parts 13, 14, 16, and 17. To effectively manage legal matters, AGC uses the Case and Document Management System (CDMS), which captures and tracks all activities and documents related to AGC legal matters.

The FAA is publishing this Privacy Impact Assessment (PIA) for the CDMS in accordance with Section 208 of the [E-Government Act of 2002](#). This assessment is necessary because the system processes Personally Identifiable Information (PII) from members of the public which includes, but is not limited to, pilots, air passengers, law firm attorneys, parties involved in legal matters, including mediation processes, designated United States (U.S.) agents for airmen with foreign addresses, and requesters of information under the Freedom of Information Act (FOIA) related to FAA legal matters.

### 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.<sup>1</sup>*

*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*

---

<sup>1</sup>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 FAA AGC uses CDMS to streamline its workload by tracking and capturing activities related to AGC matters.<sup>2</sup> More than 300 FAA AGC employees and contractors use CDMS in the following practice areas: legislation, international law, personnel and labor law, general law (i.e., Freedom of Information Act/FOIA), privacy, records management, Federal Advisory Committee Act, and ethics) regulatory enforcement, rulemaking, litigation, acquisition and commercial law, real estate, intellectual property, airport, environmental law and in-house administrative adjudications. Additionally, AGC may document administrative support activities within CDMS such as internal personnel actions, budget formation, Government Accounting Office (GAO) audit and evaluation activities, the FAA Hotline, and Office of Special Counsel matters.

With the implementation of the single, integrated platform, CDMS helps AGC to more effectively fulfill its mission by enhancing organization, collaboration, and transparency. CDMS allows AGC to streamline its work activities, increase overall staff and practice area productivity, provide spontaneous tracking and productivity reporting, and increase efficiency and value in the delivery of legal services. In addition, the integrated document and record management functionality within CDMS allows the AGC to meet the new electronic document submission requirements of the National Archives and Records Administration (NARA).

AGC generates new matters in CDMS in three ways. First, AGC users create matters in CDMS. Second, AGC services receives a request through an intake portal accessible to

---

<sup>2</sup> Matters are considered legal cases or issues that could potentially become legal cases.



certain FAA employees. Finally, FAA personnel may submit information to CDMS through FAA's Enforcement Information System (EIS).

### *Creating a New Matter*

To create a new matter, an AGC user—such as an FAA attorney, contractor, or support staff member like a paralegal—enters the name of the person involved (i.e., Smith v. FAA), a description of the legal matter, the region, and the subject. The user can also upload related documents. After the matter is created, CDMS assigns a unique tracking number and an AGC user to handle the case.

AGC users convert specified paper documents to electronic format and load them into CDMS as artifacts. These artifacts, which are uploaded into CDMS, may include pleadings, discovery materials, motions, briefs, exhibits, interrogatories, inter-office communications, a Letter of Investigation (LOIs), and memoranda. And, for in-house adjudications, artifacts may include the administrative record, decisions and orders. These documents may contain information on airmen or other members of the public (individuals involved with a legal matter). This PII may include: the name, date of birth, Social Security Number (SSN), airmen certificate number, business and personal contact information (email, address, phone, fax), medical information, results of drug tests, Enforcement Investigation Record number, violation status/type, recommended action, criminal history, aircraft information (such as aircraft registration number, registered owner), designated U.S. agent contact information (name and address), TIN/ EIN, CDMS matter number, Financial/banking information, Employment and Payroll records. The FAA then uses CDMS to manage the entire case throughout the lifecycle of the legal matter. Most of what is maintained in CDMS is in electronic format. The FAA does maintain some paper documents in locked, access-controlled filing cabinets located in the division in which the action occurred until the documents are destroyed in accordance with the appropriate retention schedule.

### *Intake Portal Requests Restrictions*

Access to legal matters within CDMS is limited depending on the nature of the matter. Generally, access is restricted to FAA employees in a particular office, division, or branch. For example, airport and environmental staff have access to airport and environmental matters, but not to personnel or enforcement matters. For some sensitive matters involving AGC employees, only the attorney assigned to the matter and their manager will be able to see the matter or access information in the matter. For some practice areas, CDMS records the name of the individual involved in the legal action in an electronic "address book," which is searchable upon manual entry by a FAA attorney or staff. Information in the address book includes the name, company or court name, business address, business phone number, and business email address of attorneys and any court officials involved in that specific legal matter. This information is specific to each legal matter, and only users assigned to that legal matter can access information on that legal matter.



### Enforcement Information System (EIS)

Most enforcement cases enter CDMS automatically from EIS. CDMS does not maintain the official records for the information shared by EIS, as the data is comprised only of copies of selected case information within EIS. The PII transmitted from EIS to CDMS may include the individual's name, date of birth (DOB), SSN<sup>3</sup>, airman certificate number, address, email address, phone number, alleged regulations violated, and recommended sanction type. CDMS receives SSNs from EIS because SSNs are included within the documents it receives. There is no SSN data field in CDMS, and SSNs are not collected directly from individuals nor entered into CDMS in any retrievable format.

### Airman with Foreign Addresses

Some airmen have a foreign address of record. The FAA now requires that certain suspected violations or investigations involving an airman with a foreign address require a designated U.S. agent and an address on file. The FAA has had difficulty reaching these airmen about specific violations or investigations. When a violation or investigation is identified, the FAA sends a LOI to the airman. Once legal action is initiated against an airman with a foreign address and there is no response to the LOI, the FAA will take further steps. The FAA will send a separate letter providing another opportunity for the airman to elect a designated U.S. agent for service of process. The designated U.S. agent's name and address can be provided to either the FAA investigating office in response to the LOI or the enforcement division attorney in response to that office's letter. The contact information may be submitted in print or by email. If collected by the investigating office, the information will be stored in the EIS's electronic Enforcement Investigation Record (eEIR), which is kept on each office's shared drive. All program offices are currently conducting investigations.

### Civil Right Mediation

The Civil Rights Scheduling Application (CRSA) is used to schedule and manage the mediation process with the aggrieved party. A CRSA user will create a case by inputting the name, email, region (city and state), phone number, and case number, for complaints that have opted in for Alternative Dispute Resolution (ADR), also referred to as a mediation request. The system will then send a dispute resolution agreement to the aggrieved party for signature through CRSA. The CRSA user will then coordinate availability of a mediator and the parties to schedule the mediation event. Once a time is selected, a meeting invitation is sent from CRSA to all parties along with a confirmation of mediation form. After the mediation event is held, details about the outcome of the event will be captured in CRSA.

---

<sup>3</sup> Although SSNs may be present in CDMS, the system does not collect the SSN directly from individuals. CDMS maintains SSNs that are contained in records that are received from data exchanges with other systems. They are used by AGC to confirm the identity of individuals who are part of a case that AGC is working on.



## 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<sup>4</sup>, 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<sup>5</sup>.*

## 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.*

CDMS is a privacy sensitive system because it maintains, uses, and disseminates PII from individuals (FAA employees/contractors, and members of the public) that are associated with an FAA legal matter. Some of the records contained in CDMS may be copies of records from other systems, such as EIS, and are thus covered under those specific system's privacy documentation including System of Records Notices (SORNs). Records in CDMS may be retrieved and accessed by unique identifiers including name and matter name.

The FAA maintains the records for the primary purpose of the system subject to the Privacy Act in accordance with the following Department's published SORNs:

Administrative Division (AGC-10)

[OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standards Act \(FLSA\) Claims and Complaints](#) 87 FR 5874

Employment & Labor Law (AGC-100)

[MSPB/Govt 1-Appeals and Case Records](#), 77 FR 65206, on October 25, 2012

[EEOC -1-Age and Equal Pay Act Discrimination Case Files](#) 81 FR 81116

<sup>4</sup> <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

<sup>5</sup> <https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final>



Aviation Litigation Division (AGC-300)

[DOT/FAA 816 - Tort Claims and Personal Property Claims Record System](#) 65 FR 19522

[DOT/FAA 821 – Litigation Information Management Systems](#) FR 19522

[DOT/FAA 847 - Aviation Records on Individuals](#) 76 FR 68849

Information Law Division (AGC-400)

[DOT/ALL 17 - Freedom of Information Act and Privacy Act Case Files](#) 84 FR 4605

Airport & Environmental (AGC-600)

[DOT/FAA 827 - Environmental Litigation Files](#) 65 FR 19476

Office of Dispute Resolution (AGC-70)

[DOT/FAA 858 Adjudication Docket Records in Aviation Litigation Proceedings](#) 88 FR 78469

Office of Civil Rights (CSRA)

[DOT/ALL 24 Department Office of Civil Rights System](#) 76 FR 71108

### **Access and Audit**

The FAA retrieves access records in CDMS by unique identifiers including name and matter name and protects Privacy Act records in accordance with Department published SORN: [DOT/All 13 - Internet/Intranet Activity and Access Records](#) 88 FR 30758 (May 7, 2002)

In addition, the CDMS may include LOIs related to violations or investigations concerning airmen. These letters are received from EIS via a data exchange. Airmen receive a Privacy Act Statement (PAS) with their LOI that explains the purpose and uses of collecting their PII. However, the LOI issuance process occurs outside of CDMS. Lastly, the publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the CDMS system.

### **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 with reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.*

The information in the CDMS is not collected directly from individuals. It comes from manual entries and data exchanges with other FAA systems. The data that comes from EIS



via a data exchange can be voluntarily updated and corrected by the individual directly in the EIS. Once the data is updated in EIS, the updated data is sent to CDMS.

CDMS functions as a repository for official administrative case records. Within CDMS, administrative records for a case can be retrieved by using the individual's name and docket number. Published decisions and orders can be retrieved from the FAA website by using the final order number.

Under the provisions of the Privacy Act, individuals may request searches to determine if any records are maintained in the system that may pertain to them. Individuals wishing to know if their records appear in a system may inquire in person or in writing to:

Federal Aviation Administration

Privacy Office

800 Independence Ave. SW

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.

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

Federal Aviation Administration

Privacy Office

800 Independence Ave. SW

Washington, DC 20591

Additional information about the Department's privacy program may be found at [www.transportation.gov/privacy](http://www.transportation.gov/privacy). If you have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at [privacy@faa.gov](mailto:privacy@faa.gov) or 1 (888) PRI-VAC1



## Purpose Specification

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

The PII in CDMS, such as name, address, DOB, SSN, Airmen Certificate number, Company name, Business and personal contact information (email, address, phone, and fax), medical information such as medical records about the airmen's health and medical profile/workup, results of drug tests, banking information (account/routing numbers), Enforcement Investigative report number (EIR), including criminal history, TIN, EIN, CDMS matter number, case number, position, title/grade, branch/unit, and employment status, is used to capture, manage, and track all activities and documents related to AGC legal matters throughout the case lifecycle. AGC uses the SSN to confirm the identities of individuals involved in a case.

CDMS operates under the following authorities:

- [Title VII of the Civil Rights Act of 1964 \(Pub. L. 88-352\) \(Title VII\), as amended](#) Covers discrimination in federally assisted programs, established a Commission on Equal Employment Opportunity, and address other related issues.
- [Age Discrimination in Employment Act of 1967 \(Pub. L. 90-202\) as amended, volume 29 of the United States Code \(U.S.C.\)](#) This act prohibits age discrimination in employment.
- [Equal Pay Act of 1963 \(Pub. L. 88-38\) \(EPA\), as amended, appears in volume 29 of the USC, at section 206\(d\)](#) The EPA covers and prohibits sex-based wage discrimination between men and women in the same establishment who perform jobs that require substantially equal skill, effort, and responsibility under similar working conditions.
- [Fair Labor Standards Act of 1938](#) Covers the establishment of fair labor standards in employment and affecting interstate commerce, and for other purposes.
- [49 U.S.C. § 40122. Federal Aviation Administration Personnel Management System](#) Gives the Federal Aviation Administration (FAA) special authority over how it manages its employees, allowing the FAA to use a more flexible, customized personnel system instead of strictly following the standard federal civil service rules.
- [Administrative Procedure Act of 1946 \(5 U.S.C. subchapter II\)](#) Covers how federal agencies create and enforce regulations.
- [Federal Tort Claims Act, 28 U.S.C. 1671, et seq.](#) Is a U.S. federal law that waives the government's usual protection from lawsuits in most cases where a private person would be liable for harm caused by a federal employee's negligence or wrongful act.
- [Military Personnel and Civilian Employees Claims Act of 1964, 31 USC 3701, 3721.](#) Is a U.S. federal law that waives the government's usual protection from lawsuits in most



cases where a private person would be liable for harm caused by a federal employee's negligence or wrongful act

- [National Environmental Policy Act of 1969, 42 SC 4321](#) Establishes a national policy for the environment effects of their proposed actions.
- [Airport Environmental Requirements, 49 USC 47106](#). The U.S. Department of Transportation (DOT) must satisfy certain environmental and community considerations before approving an airport development project grant
- [FAA Reauthorization Act of 1996, Pub. L. 104-264](#) Contains provisions on areas including the FAA's organizational structure, controller staffing and aviation workforce, modernizing the national air space system (NAS) and supporting safety and efficiency for both conventional users and new entrants.
- [Procurement Integrity Act, 41 USC 2101-2107](#) Aims to prevent corruption and ensure fair competition in government contracting by prohibiting unauthorized disclosures and establishing penalties for violations.

#### **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 minimizes data maintenance, use, and retention in CDMS to only information which is relevant and necessary for its authorized business purpose as a repository for all AGC case files. CDMS receives records from other FAA systems but only obtains information needed by AGC to fulfill its mission of providing legal support to the FAA. Once a document becomes part of the official case file, it is managed according to the associated retention schedule and is not considered a convenience copy. Thus, CDMS maintains records containing PII only when necessary to accomplish its mission. These records are subsequently destroyed in accordance with the retention schedule discussed in Appendix A.

Some of the records within CDMS, i.e., records coming from EIS, are only copies of airmen records that are used by CDMS for litigation and to process FOIA requests. EIS maintains the official copies of these airmen records and are thus covered under the applicable SORN(s) for EIS.

Information about users of CDMS including login credentials, audit trails, and security monitoring are retained until business use ceases in accordance with [NARA GRS 3.2, January 2023, Information Systems Security Records, System Access Records](#). For the applicable record retention schedules for all other records in CDMS, please see Appendix A at the end of this PIA.



## 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.*

CDMS contains the PII related to FAA employees, contractors, and members of public including pilots, air passengers, law firm attorneys, complainants, and FOIA requestors associated with FAA legal matters. This PII in CDMS is used solely for identification and case management purposes. SSNs are only utilized by the Office of the Chief Counsel (AGC) to verify the identity of individuals involved in cases they are handling. The use of the SSNs is crucial for ensuring the correct identification of individuals in legal matters. Although CDMS may contain SSNs, they are not collected directly from individuals and there is no searchable SSN field within CDMS. For case management, all other PII contained in CDMS is exclusively used by AGC for case and record management purposes by AGC throughout the lifecycle of a case.

In certain cases, AGC redacts SSNs at the attorney's discretion, in compliance with the Privacy Act and relevant FOIA exemptions. Additionally, CDMS does not use SSNs to retrieve information on matters/case files in the system. CDMS has a data exchange with the FAA's EIS system. The above individual's PII may include EIS case number, name of accused violator/equipment owner, type of violation, recommended action, name of referring manager, airman certificate number, DOB, work/personal address, and email address and phone number. Information sent to CDMS from the data exchange with EIS, such as medical or criminal information, could also be included. EIS data is used to create new legal matters within CDMS. As previously mentioned, the records sent from EIS are copies of records and EIS is the system of records for tracking information about enforcement actions for statutory or regulatory violations.

FAA limits access to this PII in CDMS to those who have a legitimate need to know and possess appropriate access credentials. Additionally, PII in CDMS is shared only with those assigned to a specific case or authorized under [DOT/FAA 847](#).

DOT discloses CDMS information outside DOT in accordance with [DOT/ALL 17 - Freedom of Information Act and Privacy Act Case Files](#) FR 4605 (February 15, 2009). Under the Freedom of Information Act (FOIA) and the Privacy Act of 1974, the Department of Transportation (DOT) maintains case files to manage records related to FOIA and Privacy Act requests, including appeals and amendments. As a routine use, all or part of the records or information contained in CDMS may be shared outside for the following purposes: identifying and providing responsive records, coordinating with other federal agencies, obtaining specialized advice, and supporting litigation and appeals.



CDMS maintains records related to position classification appeals, job grading appeals, and records concerning retained grade or pay, which are disclosed in accordance with [OPM/GOVT-9](#) (87 FR 5874) dated February 2, 2022. These records serve routine purposes, including documenting the appeals process, protecting employee rights, and ensuring compliance with federal employment laws. Records used for files in Environmental litigation are covered by [DOT/FAA 827 Environmental Litigation Files 65 FR 19476](#) (April 11, 2000). Routine includes internal agency operations to monitor and ensure compliance with environmental laws and regulations, litigation management, regulatory decision-making, and policy development. Appeals and Case records are covered by [MSPB/Govt 1- Appeals and Case Records](#), 77 FR 65206, on October 25, 2012. Routine uses cover adjudication, statutory studies, regulatory review, reporting, recordkeeping, and public access, ensuring MSPB can fulfill its statutory duties while complying with privacy and transparency requirements. Age and Equal pay case files are covered by [EEOC - 1 - Age and Equal Pay Act Discrimination Case Files](#), 81 FR 81116 (November 17, 2016). The routine uses of these files include case management and investigation, compliance monitoring, legal and remedial actions, policy development and guidance, training and education, public reporting and transparency, support for court and appeals, as well as ensuring confidentiality and privacy. Tort claims and personal property claims are covered by [DOT/FAA 816 - Tort Claims and Personal Property Claims Record System](#), 65 FR 19522 (April 11, 2000). Routine uses include investigation, reference, and court action.

PII contained in litigation and claim pleadings, discovery material, related documents (including background data on individual, or decedent involved), memoranda, correspondence, and other material used to respond to claims or prepare for litigation or hearings. The PII is retrievable by name, or the document number. Data from these files is retrieved only by people within the Office of the Chief Assistant Counsel for litigation or regional councils. These records are covered by [DOT/FAA 821- Litigation Information Management Systems](#), 65 FR 19522 (April 11, 2000). Additionally, a memorandum of understanding (MOU), dated October 31, 2019, details all the terms and conditions of the data exchange between CDMS and EIS.

### **Data Quality and Integrity**

*In accordance with 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 FAA supports the accuracy, relevance, timeliness, and completeness of information contained in CDMS. AGC also has internal business processes to maintain the quality of data in CDMS. These processes include stale dates, reminder tasks and events, and error messages where a required data field is needed for a record to save. Additionally, some PII is manually entered into CDMS by the program to begin a matter in the system. If there is an



inconsistency in the information being entered verses what is already contained in CDMS, a CDMS administrator manually looks into the EIS system, compares the information, and resolves the inconsistency. CDMS also contains business workflows and auditing functions that ensure that all PII contained in CDMS is protected. Although the PII contained in CDMS is not collected directly from the individual, the data that comes from EIS via a data exchange, can be updated and corrected voluntarily and directly by the individual directly in the EIS system. Once the data is updated in EIS, the updated data is sent to CDMS. An MOU covers the data transfer between the CDMS and EIS systems.

### 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, unauthorized access, destruction, usage, modification, and 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 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 2020 (includes updates as of Dec. 10, 2020).

CDMS is PIV-enabled. A data exchange with FAA's MyAccess system, facilitates access to CDMS. If MyAccess is unavailable, the system can also accept User ID and password for each user. Two-Factor Authentication is required if MyAccess is temporarily unavailable. Two-factor authentication is a second layer of security that prompts the user to enter a code sent to their email and/or mobile device. Sharing rules and role-based access controls are used to control user's access to data.

The FAA limits the use of PII in CDMS by appropriate access controls based on user roles for the CDMS program users and other authorized employees of the FAA who have a need to know the information for FAA business purposes. In addition, as noted above, for some sensitive matters involving AGC employees, only the attorney assigned to the matter and their manager will be able to see the matter or access information in the matter. CDMS users are also provided with system-based training, as well as a user guide for CDMS that provides guidance on proper usage of the system to reduce the possibility of inappropriate use of CDMS or the information it processes.



CDMS users are required to have necessary clearances and complete annual security and privacy awareness training and role-based training before access is allowed, or to maintain access. Access to CDMS is limited to those with appropriate security credentials, an authorized purpose, and a 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.

Additionally, CDMS has gone through a cybersecurity assessment and was issued a three-year Authorization to Operate (ATO). CDMS is reevaluated in annual security reviews. The ATO is reviewed and updated based on the outcome of security testing and evaluation in accordance with FISMA.

Lastly, all cases files, including uploaded artifacts and attachments, reside in an encrypted database. The data is encrypted at rest and while in transit.

#### **Accountability and Auditing**

*DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.*

FAA Order 1370.121, FAA Information Security and Privacy Program & Policy, implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, the FAA will implement additional policies and procedures as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with CDMS are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training, as well as FAA Order 1370.121A. The FAA will conduct periodic privacy compliance reviews of CDMS as related to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.



**Responsible Official**

Tracy Cotton  
Managing Director, Administration, AGC

**Approval and Signature**

Karyn Gorman  
Chief Privacy Officer  
Office of the Chief Information Officer

DOT Privacy Office - Approved - 05/04/2026



## CDMS PIA Appendix A

### CDMS Applicable Records Schedules

\*\*\*CDMS is the repository for all AGC case files. It's like the filing cabinet for all AGC legal matters. Once a document becomes part of the official case file, it is treated pursuant to the associated retention schedule – it is not considered a convenience copy. \*\*\*

#### Records Applicable to All Divisions

All NARA GRS referenced schedules can be found - <https://www.archives.gov/records-mgmt/grs.html>

Legal Opinion/Advice Pending schedule DAA-0237-2025-0016 is awaiting approval from NARA.

These records document the legal advice, interpretation of law, and risk assessment provided to agency officials, and may include correspondence, memoranda, and other materials prepared to guide decision-making.

The records retention period ends at the end of the calendar year, and the records are destroyed 7 years later, but longer retention is authorized if required for business purposes.

#### Formal Legal Interpretations

The records are permanent, and the retention period ends on the date of issuance.

#### Formal Legal Interpretation Rescission Memo

The records are permanent, and the retention period ends on the date of issuance.



DAA-0237-2024-001  
3\_ODRA Record Sche

Employee Management Administrative Records are covered by the [National Archives and Records \(NARA\) GRS 2.2, Employee Management Records](#) which pertains to Employee Management Records. According to schedule DAA-GRS-2017-0007-0001, Item 010, these records must be destroyed after three years; however, retention for a longer period is allowed if needed for business purposes. These records support routine office programs, administration, and human resource operations.

Financial Transaction Records are covered by the [National Archives and Records \(NARA\) GRS 1.1](#), which deals with Financial Management and Reporting Records. This schedule was approved April 2020. According to schedule DAA-GRS-2013-0001, Item 010, these records must be destroyed six years after the final payment or cancellation. However, longer retention is allowed if necessary for business purposes. These records are related to the procurement of goods and services, processing bills, collecting debts, and accounting.



Employee Incentive Award Records are governed by the [National Archives and Records \(NARA\) GRS 2.2, Employee Management Records](#), which pertains to Employee Management records. This schedule was approved in May 2024. According to Schedule DAA-GRS-2023-0002-0001, Item 30, these records must be destroyed two years after the final action; however, longer retention is permitted if needed for business purposes. These records encompass agency awards files, including recommendations, approved nominations, correspondence, and reports related to agency-sponsored cash and non-cash awards. This includes lump-sum cash awards, honorary awards, informal recognition awards, cost savings awards, and time-off awards. Additionally, the records contain correspondence regarding awards from other federal agencies, non-federal organizations, and former employees.

Procuring Goods and Services The procurement of goods and services is regulated by the [National Archives and Records \(NARA\) GRS 1.1, Financial Management and Reporting Records](#), which relates to the management of financial transactions and reporting. This schedule was approved in April 2020. According to Schedule DAA-GRS-2013-0003-0002, item 011, these records must be destroyed once the business activities have ceased.

Records supporting compilation of agency financial statement and related audit, and all records of all other reports Records that support the compilation of agency financial statements and related audits, along with all other report records, are governed by the [National Archives and Records \(NARA\) GRS 1.1, Financial Management and Reporting Records](#), which pertains to Financial Management and Reporting Records. This schedule was approved in April 2020. According to schedule DAA-GRS-2013-0003-0011, item 020, these records are to be destroyed two years after the completion of the audit or the closure of the financial statement.

#### Property, Plant and Equipment and other asset accounting

Property, Plant, and Equipment (PP&E) along with other asset accounting are governed by the [National Archives and Records \(NARA\) GRS 1.1, Financial Management and Reporting Records](#) which pertains to Financial Management and Reporting Records. This schedule was approved in April 2020. According to schedule DAA-GRS-2013-0003-0004, item 030, these records should be destroyed two years after they have assisted with the disposal of and/or removal from the agency's financial records

#### Budget Administration Records

Budget Administration Records are governed by [Nation Archives and Records \(NARA\) GRS 1.3, Budget Records](#) the GRS 1.3 which pertain to Budgeting Records. This schedule was approved December 2019. According to schedule DAA-GRS-2015-0006-0007, item 050, these records are destroyed after three years.



Budget Formulation, estimates, justification and submission records FY17 and forward

Records related to budget formulation, estimates, justification, and submissions for fiscal year 2017 and beyond are governed by the [National Archives and Records \(NARA\) GRS 1.3, Budget Records](#), titled "Budget Records." This schedule was approved in December 2019. According to Schedule DAA-GRS-2015-0006-0001, item 010, these records should be destroyed six years after the close of the fiscal year

Budget Annual Report Files

Budget Annual Report files are governed by [National Archives and Records \(NARA\) GRS 1.3, Budget Records](#). The Schedule was approved December 2019. According to schedule DAA-GRS-2015-0006-0003, item 030, these records should be destroyed when 5 years old, but longer retention is authorized if required for business use.

Position Descriptions

Position Descriptions are governed by [National Archives and Records \(NARA\) GRS 2.1, Employee Acquisition Records](#). The schedule was approved, April 2020. Records relating to developing, editing, classifying, and evaluating position descriptions, including information on title, series, grade, duties, and responsibilities. According to schedule DAA-GRS-2014-0002-0002, item 020, Destroy two years after position is abolished or superseded.

Requests for non-competitive personnel actions

Requests for non-competitive personnel actions are governed by [National Archives and Records \(NARA\) GRS 2.1, Employee Acquisition Records](#). The schedule was approved, April 2020. According to schedule, DAA-GRS-2014-0002-0013, item 080, Destroy one year after approval is granted or denied.

Employee Emergency Contact Information

Employee emergency contact information records are governed by the [National Archives and Records \(NARA\) GRS 5.3, Continuity and Emergency Planning Records approved March 2022](#). According to schedule, DAA-GRS-2016-0004-0002, item 020, destroy when superseded, obsolete or upon separation or transfer of employee.

Continuity Planning and Related Emergency Planning Files

Continuity planning and related emergency planning files are governed by [National Archives and Records \(NARA\) GRS 5.3, Continuity and Emergency Planning Records approved March 2022](#). According to schedule, DAA-GRS-2016-0004-0001, item 010, destroy when three years old or three years after superseded or obsolete.

**AGC 70 – OADRA**

Civil Penalty Hearing Docket Records



DAA-0237-2024-0013 This schedule is awaiting NARA's approval.

**Original Docket Files or Records Not Optically Scanned by DOT Docket Management System**

[Civil Penalty Hearing Dockets N1-237-00-1](#), Item 1(a)

The record retention period concludes at the end of the fiscal year. Records are transferred to the Federal Records Center (FRC) several months later and are destroyed five years after transfer.

**Original Docket Files or Records That Have Been Optically Scanned by DOT DMS [N1-237-00-1](#), Item 1(b)**

After the case file is resolved and closed, retain the paper records for at least 30 days following optical scanning and verification of the imaging. Destroy case files no later than one year after closure.

**Records That Have Been Optically Scanned but Originals must be Retained (photographs, charts, etc. if needed by Agency)**

[N1-237-00-1](#), Item 1(c)

The record retention period ends at fiscal year-end, and the records are transferred to the Federal Records Center (FRC) three months after and destroyed 5 years after the transfer to FRC.

**Optical Disk DOT Docket Management System (DMS) Copy of Civil Penalty Hearing Docket Files or Records**

[N1-237-00-1](#), Item 1(d)

These records are temporary and should be deleted or erased five years after the Civil Penalty docket file closes.

AGC 100 Employment and Labor Law

Alternative Dispute Resolution Records (informal) Alternative dispute resolution (ADR) case files are governed by the [National Archives and Records Administration \(NARA\) GRS 2.3, Employee Relations Records approved May 2024](#). According to schedule DAA-GRS-2018-0002-0007, item 070, Destroy these records three years after the case is closed. Retain them longer if required for business purposes.

Reasonable Accommodation Case Files- formal

Reasonable accommodation case files are governed by the [National Archives and Records Administration \(NARA\) GRS 2.3, Employee Relations Records](#). According to schedule DAA-GRS-2022-0001-0002, item 020, these records should be destroyed three years after an employee's separation from the agency or after all appeals are concluded, whichever is later, but longer retention is authorized if required for business use.



### EEO Official Discrimination Complaint Case Files - informal

EEO discrimination complaint case files are governed by the [National Archives and Records Administration \(NARA\) GRS 2.3, Employee Relations Records](#). According to schedule,

DAA-GRS-2018-0002-12, item 110, these records should be destroyed three years after resolution of case, but longer retention is authorized if required business use.

### EEO Official Discrimination Complaint Case Files – formal

EEO official discrimination complaint case files (formal) are governed by the [National Archives and Records Administration \(NARA\) GRS 2.3, Employee Relations](#). According to schedule DAA-GRS-2018-0002-0013, item 111, destroys these records seven years after resolution of case, but longer retention is authorized if required for business use.

### Merit System Protection Board and Federal Litigation Adverse Action

Merit system protection board (MSPB) case files are governed by the [National Archives and Records Administration \(NARA\) GRS 2.3, Employee Relations Records](#). According to schedule DAA-GRS-2018-0002-0009, item 080, destroy three years after final resolution of case, but longer retention is authorized if required for business use.

[Litigation Action Files N1-237-91-2](#) The disposition authority associated with NARA states that Litigation action files are to transfer to the federal records center (FRC) three years after the case is closed and destroyed 13 years after the case is closed.

## **AGC 200 – Regulations (all Subdivisions)**

### Legal Opinion /Advice

These records document the legal advice, interpretation of law, and risk assessment provided to agency officials, and may include correspondence, memoranda, and other materials prepared to guide decision-making.

Pending schedule DAA-0237-2025-0016 is awaiting approval from NARA.

The retention period ends at the end of the calendar year. Records are destroyed 7 years after the retention period ends, but longer retention is authorized if required for business purposes.

## **AGC 300 Enforcement (all subdivisions)**

### Legal Enforcement Case Files

Pending schedule awaiting approval from NARA: DAA 0237-2025-0005

The retention period ends when the case is closed. For case files with no action, destroy them five years later.



[N1-237-92-4](#), Item 1 The disposition authority associated with NARA states that case files resulting in no action should be destroyed 30 days after case closes in EIS.

Case files resulting in indefinite suspension of an airman certification pending successful completion of reexamination or proof of qualification

[N1-237-92-4](#), Item 1 The disposition authority associated with NARA states records should be destroyed 1 month after successful completion of reexamination or proof of qualification.

#### Violation Report Files

[NC1-237-77-3](#), Item 87 The disposition authority associated with NARA states records should be destroyed in agency when no longer needed.

#### **AGC 400 Litigation and General Law**

Pending scheduling awaiting approval:

The retention period ends at the end of the calendar year. Records are destroyed 7 years after the retention period ends, but longer retention is authorized if required for business purposes. DAA-0237-2025-0016

#### **AGC 500 Contracts and Litigation**

Pending schedule awaiting approval from NARA: DAA-0237-2025-0016

#### **AGC 600 – Airports and Environmental**

Pending schedule awaiting approval from NARA: DAA-0237-2025-0016

#### **AGC 800 – Legislation**

Schedule is revised and will be superseded by: DAA-0237-2025-0011

#### **Legislative Legal Advice Record**

These records are temporary. According to DAA-0237-2025-0011 Disposition, the retention period ends when the matter is inactive. Destroy records fifteen years later.

#### **FAA Legislative Proposal Legal Advice Records**

These records are Permanent. According to DAA-0237-2025-0011 Disposition, the retention period ends at the end of the current session of Congress



## **AGC 900 Ethics**

### **Financial Disclosure Reports**

#### **OGE Form 450**

Confidential Financial disclosure reports are governed by the [National Archives and Records Administration \(NARA\) GRS 2.8, Employee Ethics Records](#). According to schedule DAA-GRS-2014-0005-0012, item 071 records should be destroyed six years after the agency receives the OGE Form, unless the OGE Form 450 supports one or more subsequent optional OGE Form 450s.

#### **OGE Form 278**

According to schedule DAA-GRS-2014-0005-0009, item 062 should be destroyed 7 years after it is received by the agency.

### **Ethics Program Review Records**

[National Archives and Records Administration \(NARA\) GRS 2.8, Ethics Program review Records](#) Reports of payments accepted from non-federal sources. According to DAA-GRS-2014-0005-0006, item 050, records should be destroyed six years after all outstanding deficiencies in the ethics program review have been resolved.

Item 030 Reports of Payments accepted from non-Federal sources records are temporary and should be destroyed 3 years following submission of the report to OGE, but longer retention is authorized if required by business use. DAA-GRS-2014-0005-0003