



Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 563
System Name: CBCA Electronic Docketing Application
CPO Approval Date: 10/19/2026
PIA Expiration Date: 10/18/2029

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
CBCA Electronic Docketing Application

B: System, application, or project includes information about:

C: For the categories listed above, how many records are there for each?

D: System, application, or project includes these data elements:

Overview:

The Electronic Docket System (EDS) is a web-based Information Technology (IT) platform that supports the quasi-judicial mission of the Civilian Board of Contract Appeals (CBCA). Serving as a central computing environment for CBCA judges and personnel, EDS provides a unified hub for managing and processing case-related applications and operations. The system facilitates the processing, storage, and transmission of sensitive administrative and litigation data involving contract disputes between government contractors and executive agencies. While hosted externally, EDS is integrated with the GSA network and remains accessible to CBCA staff as well as agency and public litigants.

B. System, application, or project includes information about:

Federal employees (CBCA judges and administrative staff), government contractors, legal representatives, and members of the public acting as active litigants or registrants within official contract dispute proceedings.

C. For the categories listed above, how many records are there for each?

1. CBCA Personnel / Internal Users: Less than 200 active records.

2. External Litigants / Public Registrants: Approximately 1,000 to 5,000 historical and active records (supporting ongoing case tracking growth parameters).

D. System, application, or project includes these data elements:

Full Name, Business/Personal Email Address, Telephone Number, Physical Mailing Address, Job Title, Company/Agency Affiliation, Case Docket Numbers, and associated legal identifiers embedded voluntarily within case pleadings and filing attachments.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
Contract Disputes Act, 41 U.S.C. §§ 7101-7109

Section 423 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), 42 U.S.C. § 5189a(d), as amended by Section 1219 of the Federal Aviation Administration Reauthorization Act of 2018, Pub. L. 115-254

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?
New SORN required

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?

That system includes information about Federal employees, contractors, and members of the public contained in case filings. The system maintains just one category of information – administrative data. This data, which is used for the filing and processing of cases, can include the parties' voluntarily submitted names and contact information (for example, telephone number, mailing address, and email address) and other information necessary to resolve the dispute at issue.

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.

The records retention schedule for the Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) enforces a tiered lifecycle management process:

- Tier 1 Active Online Lifecycle:
Case documentation, docket entries, and user account metadata remain hosted active and online in the production database tier for exactly 180 days following official case closure.
- Tier 2 Offline Archival Retention: Upon reaching the 180-day post-closure threshold, the Clerk of the Board executes a manual data migration sequence. All case pleadings, flat PDF filings, and related tracking sheets are compiled into an archive bundle and moved to an access-restricted, offline CBCA drive for a mandatory 5.6-year retention hold. When the case files are deleted, the matching relational database rows are deleted from the backend Microsoft SQL Server database schemas.
- Tier 3 Absolute Destruction: Once the 5.6-year archival lifecycle expires, all offline files are permanently deleted.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?

The collection of a limited set of self-asserted PII (specifically Full Names, Business/Personal Email Addresses, Telephone Numbers, and Physical Mailing Addresses) is operationally and legally necessary to fulfill the quasi-judicial mission of the Civilian Board of Contract Appeals (CBCA) under the Contract Disputes Act.

First, this data is required to establish unique public user accounts, verify user identity at login, and map individuals to their specific legal proceedings, which ensures that unauthorized parties cannot access or alter sensitive case files (AC-03).

Second, the system uses email addresses to execute automated docketing notification loops. This satisfies legal notification requirements by immediately alerting active litigants whenever an order, pleading, or scheduling change is issued in their case. Without this core collection, the system could not maintain reliable communication channels, execute due process, or securely restrict case file access to authorized participants.

3.2: Will the system, application, or project create or aggregate new data about the individual?

No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

Data blocks are compartmentalized using strict database relational controls and Application-level Role-Based Access Control (RBAC). Network transit is encrypted end-to-end using forced TLS 1.2 / TLS 1.3 protocols on Port 443. Backend system administration and folder paths are completely hidden behind a Zero Trust perimeter utilizing Zscaler Private Access (ZPA). Privileged server shell interactions over Remote Desktop Protocol (RDP) strictly require a GSA Short-Name Account (SNA) credential combined with a physical SNA hardware multi-factor token.

3.4 Will the system monitor the public, GSA employees, or contractors?

None

3.4 Explain: Please elaborate as needed.

The system does not monitor individual behavior, web history, or public activities. It exclusively logs standard, forensically auditable application event metrics (such as login timestamps, account modification transactions, and file upload milestones) to comply with federal security audit mandates.

3.5 What kinds of report(s) can be produced on individuals?

- **Authentication History:** Reports exactly who logged into the system and when, tracking the precise timestamps of each user session.
- **File Ingestion Activity:** Documents what files were uploaded and when, providing a complete compliance record for all flat PDF case document filings.
- **Organizational Affiliation:** Tracks the specific agency or litigation party they work for to enforce role-based access limits.
- **Account Lifecycle Lineage:** Audits the full historical state timeline of user accounts as they transition from new, to active, down to deleted status values.

3.6 Will the data included in any report(s) be de-identified?

No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?

CBCA does not produce reports on individuals.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?

Other Individuals

4.2How: If so, how will GSA share the information?

4.3: Is the information collected:

Directly from the Individual

4.3Other Source: What is the other source(s)?

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?

No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?

No

4.4NoAgreement: Why is there not a formal agreement in place?

There is no formal external sharing agreement in place because the Electronic Docketing System (EDS) is a brand-new application currently going through its very first initial Assessment and Authorization (A&A) process.

- Initial Authorization Phase: As a newly deployed system boundary, EDS is currently establishing its official security and privacy baselines to achieve its first formal Authorization to Operate (ATO).

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

The system only collects PII from users necessary to create an account in EDS that is tied to a litigant in a case before the Board. Each user controls the accuracy of the information they provide.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?

Authorized citizen litigants, legal representatives, CBCA Board clerks, and privileged system administrators who maintain the underlying middleware layer.

6.1b: What is the authorization process to gain access?

The Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) utilizes a multi-factor authentication pipeline to authorize user access. The process is being updated from a legacy system account model to a modern, federated federal single sign-on model:

1. Legacy Registration and Verification Process (Pre-Upgrade Baseline)

Initially, a user navigated to the EDS landing page and clicked "Register as a New User". The user completed a profile form with a valid email address and interactively checked a box to formally accept the Rules of Behavior (RoB). The system then generated a temporary password and sent it to the user's registered email. Upon initial login with these credentials, the system intercepted the session and forced a mandatory new/change password request. To grant access, the new password had to pass federal complexity checks requiring 12 to 24 characters containing at least one uppercase letter, one lowercase letter, one number, and one special character.

2. Modern Login.gov Verification Process (Current Upgrade Deployment)

Under the modernized architecture baseline, the authorization gate is completely offloaded to the federal Login.gov Identity Provider (IdP) gateway. To gain system access, a user lands on the portal page, interactively accepts the mandatory GSA System Use Notification and public privacy banners, and clicks the blue "Sign in with Login.gov" button. The frontend application redirects the browser directly to the secure Login.gov perimeter, where the user must

provide their credentials and successfully clear mandatory AAL2 multi-factor authentication challenges (such as an authenticator app token or hardware security key).

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?

Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?

Physical: Hosted within a secure, FedRAMP Moderate authorized virtual cloud data center facility protected by physical biometric locks, continuous guard boundaries, and strict asset surveillance.

Technical: Employs automated IntelliJ static linter inspections, SonarQube pre-commit code gates to eliminate text manipulation vulnerabilities, isolated Microsoft SQL databases over internal Port 1433 channels, and end-to-end Zscaler network micro-segmentation.

Managerial: Enforces mandatory annual GSA privacy and security awareness training for all users, mandates formal ServiceNow change management tickets for any code deployment, and operates under strict Rules of Behavior validation controls.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?

Yes

6.4What: What are they?

CBCA follows GSA procedures in place for handling security incidents. CBCA and GSA monitor use of its systems and is responsible for reporting any potential incidents directly to the CBCA's Information Systems Security Officer. This Officer coordinates the escalation and reporting to GSA, and the Board's response procedures.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?

Users must provide basic contact information in order to access EDS.

7.1Opt: Can they opt-in or opt-out?

No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

The submission of data by the parties is purely voluntary. To protect sensitive details from public disclosure, parties have the option to seek a protective order or submit specific data *in camera*, restricting access solely to designated individuals and the presiding judges.

7.2: What are the procedures that allow individuals to access their information?

Parties submit case-related data, which may subsequently be amended by filing a motion with the presiding judge.

7.3: Can individuals amend information about themselves?

Yes

7.3How: How do individuals amend information about themselves?

Parties submit case-related data, which may subsequently be amended by filing a motion with the presiding judge.

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

CBCA and agency users of EDS are required to attend training on what is PII and how to protect PII. Non-governmental users of EDS submit their limited personal information to the system in order to register an account. The EDS landing page warns users not to submit the following personal identifiers to the system:

Social Security Numbers, Dates of Birth, and Financial Account Numbers.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?

The System Owner enforces strict compliance with stated privacy practices through three technical and administrative control gates:

- Secure Development Builds: Code changes are manually reviewed inside the IntelliJ workspace using SonarLint static linters and pre-commit gates to programmatically prevent unauthorized data collection or variable leaks before compilation.
 - ServiceNow Change Governance: Every system configuration change, and library update must be logged as a formal tracking ticket in GSA ServiceNow. Changes are frozen until they clear a formal security impact analysis and Configuration Control Board (CCB) approval.
 - Continuous Log Auditing: Sensitive user PII remains locked within the back-end Microsoft SQL Server tier. Active application access logs and account status changes stream in real time to the GSA Enterprise Logging Platform (ELP), allowing the 24/7/365 GSA Security Operations Center (SOC) to monitor, trace, and block unauthorized data use.
-