



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: 540
System Name: OGC Case Tracking
CPO Approval Date: 6/30/2026
PIA Expiration Date: 6/29/2029

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Andy Ibarra

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
OGC Case Tracking

B: System, application, or project includes information about:
The OGC Case Tracking application is used to track information for all types of claims against GSA. The Office of the General Counsel (OGC) represents the agency in all types of claims and lawsuits. These cases are recorded and

tracked in the filed in the system to record basic data. This data is used to track outcomes of cases and produce reports for audits.

The Personnel Cases for the OGC Case Tracking application handle sensitive information for cases involving GSA employees. Personnel cases can involve lawsuits with GSA employees. For this reason, the visibility and access for personnel cases must be low and only certain attorneys and managers should be able to access these cases. The OGC application will handle personnel and non-personnel case tracking with a security structure that will allow access to certain cases and limit access to specified personnel attorneys in each GSA region.

C: For the categories listed above, how many records are there for each?
1,000 Cases

D: System, application, or project includes these data elements:
First Name, Last name, business email, business and personal phone numbers

Photos drawings and videos of government buildings

Overview:

The OGC Case Tracking application is used to track information for all types of claims against GSA. The Office of the General Counsel represents the agency in all types of claims and lawsuits. These cases are recorded and tracked in the filed in the system to record basic data. This data is used to track outcomes of cases and produce reports for audits.

The Personnel Cases for the OGC Case Tracking application handle sensitive information for cases involving GSA employees. Personnel cases can involve lawsuits with GSA employees. For this reason, the visibility and access for personnel cases must be low and only certain attorneys and managers should be able to access these cases. The OGC application will handle personnel and non-personnel case tracking with a security structure that will allow access to certain cases and limit access to specified personnel attorneys in each GSA region.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
28 U.S.C. §§ 471-482

Federal Rules of Civil Procedure

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?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
GSA/OGC-1, Office of General Counsel Case Tracking and eDiscovery System

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.

OGC retains records pursuant to the retention schedule promulgated by NARA. Information is retained indefinitely as is necessary for retaining the documentary records of OGC's continuous representation of the Agency. The system stores and organizes key data points regarding every claim and litigation matter handled by OGC.

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? No

2.1 Explain: If not, please explain.

OGC Case Tracking is not external to GSA and is only accessible by authorized users from the GSA Office of General Counsel. OGC Case Tracking does not collect personal information directly from individuals. Point of Contact Information stored within OGC Case Tracking is optional and is entered in manually by authorized users of the OGC Case Tracking System.

3.0 Data Minimization

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

OGC Case Tracking does not collect PII. Claims that are stored within OGC Case Tracking is necessary for the Office of General Counsel (OGC) to handle sensitive information for cases involving GSA employees.

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?

OGC Case Tracking is not external to GSA and is only accessible by authorized users from the GSA Office of General Counsel. Users are required to have their account requested and approved via ServiceNow based on their need to know. RBAC access is in place to limit user access to data to that is only needed for their role and function. GSA Auth is used for authentication.

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

None

3.4 Explain: Please elaborate as needed.

N/A. The system is not used as a monitoring tool.

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

N/A. Reports are generated on individuals.

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?

N/A. Reports are generated 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?

None

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

N/A

4.3: Is the information collected:
From Another Source

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

OGC Case Tracking is not external to GSA and is only accessible by authorized users from the GSA Office of General Counsel. OGC Case Tracking does not collect personal information directly from individuals. Point of Contact Information stored within OGC Case Tracking is optional and is entered in manually by authorized users of the OGC Case Tracking System.

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?
N/A. OGC Tracking does not share data with any other systems.

5.0 Data Quality and Integrity

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

OGC relies on their users of the OGC Case Tracking to review all data that is entered in for accuracy and completeness.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
GSA OGC Employees and Contractors.

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

To obtain access to the system, users are required to have the need to know based on their role and function within the GSA Office of General Counsel. The OGC System Tracking PM submits new user access requests via servicenow for approval before accounts are provisioned for access. All users are required to authenticate using GSA Auth.

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.
9/8/2025

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

OGC Case Tracking is only accessible to a limited number of OGC personnel, which is only accessible through GSA Auth. In addition role-based access has been implemented to only users with need-to-know. OGC Case Tracking is hosted within Salesforce. Data is encrypted at rest and in transit.

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?

In the event of suspected or confirmed security incident, OGC staff have received instruction and training to call and refer any such incident to GSA's Privacy Office for further action. The GSA Incident Response team will be alerted to investigate further.

7.0 Individual Participation

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

No opportunity exists to consent, decline or opt out. Information is collected directly from employees who handle litigation matters or administrative proceedings on behalf of GSA.

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.

No opportunity exists to consent, decline or opt out. Information is collected directly from GSA Employees and Contractors who handle litigation matters or administrative proceedings on behalf of GSA.

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

OGC Case Tracking is not the primary system of record collection, Individuals can request details regarding their claim from other sources or individuals.

7.3: Can individuals amend information about themselves?

No

7.3How: How do individuals amend information about themselves?

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.

OGC Case Tracking is an application used to manage OGC records related to litigation or administrative proceedings that GSA is involved with. All application users take an annual required Privacy Act training related to maintenance, storage and use of PII. All application users are requested to report any suspected breach of PII to the GSA IR team and the GSA IT Help desk.

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?

All GSA employees receive Privacy Act training annually and thus they are required to protect the records transferred into OGC Case Tracking per Privacy Act requirements.
