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: 434
System Name: EEO Complaint Management System (EEO CMS)
CPO Approval Date: 6/27/2023
PIA Expiration Date: 6/26/2026

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chris McFerren

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
EEO Complaint Management System (EEO CMS)

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

The OCR Complaint Management System, iComplaints will now change to ETK EEO 3.3.0 - Entellitrak - Through Tyler Technologies, Inc, includes information about: GSA federal employees and applicants for employment who are EEO complainants, representatives, witnesses, and potentially, GSA personnel involved in investigations.

C: For the categories listed above, how many records are there for each?
There are approximately 3585 unique records about GSA employees and applicants for employment who are EEO complainants as of May 2023.

D: System, application, or project includes these data elements:
EEO-CMS maintains the following information about individuals, when relevant to EEO complaint activity, within EEO Complaint Management System:
a. Name and other biographic information, including date of birth; race; national origin; sex, including pregnancy status, sexual orientation, and gender identity; religion; disability status and other medical information; genetic information; and prior EEO activity.
b. Contact information, such as home and work address; telephone numbers; email addresses.
c. Financial information related to fact-based inquiries for complaints, which may include credit card bills, credit reports; payments to medical institutions, bank transfer data for settlement or other payments from the agency. The results of complaint inquiries (direct, comparative, and statistical evidence and information from forms, sworn statements of fact, reports, and summaries) as routinely created and collected during the course of federal sector EEO complaint processing are entered and maintained in the database.

Overview:

OCR utilizes the Complaint Management System to: (1) provide for complainants to file complaints and receive updates on their case (efile module); (2) monitor and track complaints nationwide; and (3) report on nationwide complaints activity including reports to EEOC (No FEAR and QRM modules).
The annual software maintenance includes technical support, software product releases and enhancements, onsite upgrade support, annual A&A review support, security scan, custom reports and query support, custom configuration, ad hoc user and role administration support, onsite infrastructure and network support. It also includes annual system, platform, architecture and process review and recommendations by an application engineer.
The eFile module allows an unlimited number of external users, regulated by permissions, to electronically file records, submit documents related to each record, and check the status of a record. efile is a J2EE-compliant Web-based module requiring no client-side installation of any software. All processing is done on the application and database servers. This allows a larger volume of transactions to be stored without any effect on the speed of the Web browser portal where users input their data and/or view the status of individual records. The system sends email alerts to Agency staff about certain record processing activities including the filing and addition of documents. The system features user-friendly navigation and is maintained in OCR's Central Office with regional data entry.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
All data fields within the EEO Complaint Management System exist to give GSA the ability to not only identify the issues and bases of EEO complaints, the complainants, the witnesses, and other information necessary to analyze complaint activity and trends, but also to track and monitor the location, current status, and length of time elapsed at each stage of the federal sector complaint process consistent with EEOC Management Directive 110. While certain information is mandatory, other information is collected only when material is relevant to an investigation, or necessary for the preparation and submission of EEO activity reports to the EEOC and/or Congress. The information collected by this system is covered by Government-wide System of Records Notice EEOC/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeal Records.

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 Agency-1 Information is searchable by name or complaint ID only. GSA's System of Records of Notice can be found in the Federal Register at: https://www.federalregister.gov/documents/1996/11/26/96-30071/privacy-act-of-1974-system-of-records

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.
The OCR Complaint Management System does not serve an information collection-related function subject to the Paperwork Reduction Act. Consequently, OCR has not submitted an information collection request to OMB.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Specific to EEO complaint records, NARA has established standards for records retention under File #332. The Agency will remove and place cases in inactive files after resolution of the EEO case. There will be a cut off of inactive files annually. GSA will destroy case files 4 years after cutoff (GRS1, item 25a).

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?
Even without the EEO Complaint Management System, OCR would have to collect and use PII in order to fulfill its mission to provide a work environment free of discrimination and retaliation, in compliance with EEOC laws and regulations and with the No FEAR Act. OCR staff uses the PII collected and maintained in the EEO Complaint Management System to:
a. Manage and track formal and informal EEOC complaints;
b. Review the status of open cases;
c. Analyze trends with EEO activity; and
d. Prepare and submit annual reports to Congress and to the EEOC. GSA OCR is able to submit the required annual MD-715 report to Congress and the annual Federal EEO Statistical Report of Discrimination Complaints (EEOC Form 462) to the EEOC more easily using the EEO Complaint Management System. These reports include only summary level/aggregate data. OCR regularly produces for internal use only reports that include personal information on individuals.

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

3.2 Explained: If so, how will this data be maintained and used?
The EEO Complaint Management System maintains information concerning GSA staff, applicants for employment, and former employees who contact OCR to file informal and formal EEO complaints. This data is used for mandatory reporting requirements to various statutory authorities, program management/administration, and quality control.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
OCR employees are the only authorized users of the EEO Complaint Management System. Role-based access control (RBAC) is implemented in the EEO Complaint Management System to control access to the system and to prevent unauthorized use. Roles are defined for each authorized user, which prevents authorized users from accessing other parts of the system. Users are strongly authenticated to the system. The system logs unauthorized access attempts.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.

The EEO Complaint Management System does not monitor the public, GSA employees, or contractors

3.5 What kinds of report(s) can be produced on individuals?
a. Ad-hoc query reports are produced on individuals
b. The No FEAR Act Report and the EEOC Form 462 report are aggregated and do not provide information 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?
All information in the reports is de-identified.

3.6 Why Not: Why will the data not be de-identified?
No individuals are named. Data for these reports in narratives, tables, and graphics is in an aggregate form, reducing the ability to identify individuals based on pertinent criteria.

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?
If a hearing or appeal is requested, the Office of General Counsel is provided with the report of investigation and complaint file, as they defend the agency in EEO matters. Settlement agreements are shared with the Office of Human Resources Management for processing. The agency EEO director is aware of settlement agreements and high profile cases. Management officials and witnesses become aware of pending investigations for which their testimony is required. The information is also shared with GSA Heads of Service and Staff Offices (HSSOs), complainants and their representatives.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
Information from other sources is required to supplement the information provided by the individual. The information is indirectly collected as a result of the media (for example, the web form). It may include data such as timestamp, operating system, and user-agent ("browser"). Contextual data often contains information captured by GSA. The majority of data is collected Directly from the Individuals, with the remaining information being related to other records or information systems, e.g. personnel files.

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?
The system will not directly interact with other internal GSA systems or external systems. The system does produce reports that are disclosed to other agencies.

4.4Formal Agreement: Is a formal agreement(s) in place?
No

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

N/A. There are no interconnections with other external systems.

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 does produce reports that are disclosed to other agencies.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Only certain OCR staff are granted access to the EEO Complaint Management System, based on their role and responsibility within OCR.

6.1b: What is the authorization process to gain access?
All OCR staff that accesses the data has a Public Trust clearance. In accordance with GSA IT system security requirements, all requests are made using the ServiceNow system.

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.
3/25/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
GSA assesses information and systems for compliance risk, reputational risk, strategic risk, situational/circumstantial risk, and operational risk. In order to mitigate these risks to an acceptable level, GSA implements extensive security controls for information collected or maintained on its behalf, and conducts third-party assessments of vendors and services it procures. GSA implements the following controls for internally maintained systems: GSA policies and procedures governing privacy and information security; background checks on all personnel with access to the system; initial and follow-on privacy and security awareness training for each individual with access to the system; physical perimeter security safeguards; Security Operations Center (SOC) to monitor antivirus and intrusion detection software; risk and controls assessments and mitigation; technical access controls, such as role-based access management and firewalls; and appropriate disaster mitigation strategies, breach notification processes and plans, and secure channels for submitting information. GSA implements controls relevant to third party vendors and services according to risks identified for the following types of third party reviews: Third Party Security Assessment and Authorization (SA&A) Package; Statements on Standards for Attestation Engagements (SSAE) Review; Risk Assessments by Independent Organization; or a complete Risk Assessment by GSA.

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?
GSA has procedures in place for handling security incidents. GSA monitors use of its systems and is responsible for reporting any potential incidents directly to the relevant Information Systems Security Officer. This Officer coordinates the escalation, reporting and response procedures on behalf of GSA. The procedures are outlined in GSA Order 2100.1M CIO GSA Information Technology Security Policy https://insite.gsa.gov/directives-library/gsa-information-technology-it-security-policy-21001m-cio?term=2100.1L CIO CHGE 1. All OCR staff, such as federal employees, contractors, detailees, interns, or any other person performing services on behalf of OCR are responsible for immediately informing their supervisor of any potential PII incidents. OCR will take immediate, effective steps to remedy the situation in accordance with GSA policy 9297.2 CIO CIO CHGE 1 GSA Information Breach Notification Policy and OCR's Notice of Breach Confidentiality standard operating procedure. OCR's Deputy Associate Administrator or their designee shall notify GSA's Office of the Chief Information Security Officer via the GSA Office of Information Technology (IT) Service Desk within one hour of discovering the incident. Where the incident involves PII within the OCR Complaint Management System, GSA's Chief Privacy Officer must also be notified. Additionally, OCR

shall comply with the direction of the CPO, in consultation with the Office of General Counsel (OGC) on what, if any, additional steps are required.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Individuals seeking to initiate complaints or participating in the EEO complaint process are informed that their information will be used to process their complaint.

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

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
Individuals may not access their information, as the only individuals with access to the system are OCR staff.

7.2: What are the procedures that allow individuals to access their information?
Individuals can call the OCR Helpdesk, or send an email to the assigned OCR Ethics employee. Individuals can also use the eFile interface to access their information.

OCR staff amends information on their behalf. If they E-file, our office converts the information for them so an EEO employee updates the information not the actual individual.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?
No, OCR staff amends information on their behalf. If they E-file, our office converts the information for them so an EEO employee updates the information not the actual individual.

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.
GSA requires privacy and security training for all personnel and has policies in place that govern the proper handling of PII.

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?
GSA requires privacy and security training for all personnel, and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems, including those that support the EEO Complaint Management System, and has limited access to those personnel with a need to know. Further, OMB requires the GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act. As appropriate, GSA may identify individuals to act as a Contracting Officer's Representative (COR) to train third parties with whom it collaborates, and monitor third party performance. GSA proactively informs anyone who participates in the EEO Complaint Management System of its inherent privacy risks and the steps GSA takes to mitigate them. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. As discussed above, GSA takes automated precautions against overly open access controls.