OCR Complaint Management System

Privacy Impact Assessment (PIA)

July 20, 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Nate Ciano, ISSM

Name of Program Manager/System Owner:

- Mary D. Gibert, Associate Administrator

Signature Page

Signed:

DocuSigned by:
Nathaniel Ciano
113E722762814433...
Information System Security Manager (ISSM)

DocuSigned by:
Mary D. Gibert
2D506F41ED214BA...
Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183F40A...
Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0

2/20/2020	Removed email field from signature page	3.1

Table of contents

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?

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

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

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

Document purpose

This document contains important details about the Office of Civil Rights (OCR) Complaint Management System. To accomplish its mission OCR must, in the course of processing equal employment opportunity (EEO) complaints, collect personally identifiable information (PII) about the people who file EEO complaints. 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]

A. System, Application, or Project Name:

The OCR Complaint Management Systems, commonly known as iComplaints, is a commercial off-the-shelf, electronic records system used to track complaints and supporting documentation relating to individual and class complaints of employment discrimination and retaliation prohibited by civil rights statues. The OCR Complaint Management System is also used to meet EEOC data reporting requirements as set forth in the Code of Federal Regulations governing federal sector EEO Complaint processing (29 CFR parts 1614) and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No Fear Act). The OCR Complaint Management System (iComplaints) is part of GSAs (input security info), and is part of the Enterprise Architecture System (EAS) and gets its lifespan through the EAS authority to operate (ATO).

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

The OCR Complaint Management System, iComplaints, 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 3,264 unique records about GSA employees and applicants for employment who are EEO complainants as of May 2020.

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

OCR maintains the following information about individuals, when relevant to EEO complaint activity, within OCR Complaint Management System:

- 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.
- Contact information, such as home and work address; telephone numbers; email addresses.
- 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

All data fields within the OCR 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.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

The collection of information is mandated by EEOC regulations at 29 CFR Part 1614, which directs federal agencies to process complaints of alleged discrimination under the laws enforced by the EEOC. EEO Management Directive 715 (MD-715), *Essential Elements of Model Agency Programs under Title VII of the Civil Rights Act and Rehabilitation Act,* issued by the EEOC, requires that the agency use a complaint tracking and monitoring system that permits the agency to identify the location, status, and length of time elapsed at each of the agency's complaint resolution process, the issues and bases of the complaints, the aggrieved individuals and complainants, the involved management officials, and other information necessary to analyze complaint activity and identify trends.

Agencies must submit annual reports of aggregated complaints-related statistics to the EEOC and to Congress. They must also purchase and/or develop systems that can compile the necessary information to track EEO complaint activity for case management and reporting in accordance with EEOC regulations and MD-715. https://www.eeoc.gov/federal/directives/md715.cfm

1.2 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information?

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

1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

No. 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 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

Yes. 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).

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Yes. Individuals are given notice of how information collected in the OCR Complaint Management System may be used through the following statement on OCR's website located at https://akassistant-pd.gsa.gov/efile-gsa-prod/login/:

"*The authority for collecting this information is 49 U.S.C. 114, and 42 U.S.C. 2000e-16(b) and (c). Purpose: This information is needed to initiate the employee web-based EEO complaints. Disclosure: Furnishing this information is voluntary; however, failure to provide it will delay electronic processing of your complaint. Routine Uses: This information may be disclosed to individuals that have a need to know the information in the performance of official duties associated with providing assistance in processing EEO complaints. This information may also be shared pursuant to the Privacy Act System of Records EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records (July 30, 2002, 67 FR 49338).*"

However, EEO complaints and eFile typically do not rely on directly identifying PII for analysis. To the extent that GSA seeks to publish or share information that directly identifies individuals, it will first seek the individual's consent. All other EEO complaint-related information is otherwise shared in an aggregated form to limit individual identification.

SECTION 3.0 DATA MINIMIZATION

GSA limits PII collection only to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

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

Even without the OCR 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's staff uses the PII collected and maintained in the OCR Complaint Management System to:

- Manage and track formal and informal EEOC complaints;
- Review the status of open cases;
- Analyze trends with EEO activity; and
- 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 OCR 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? If so, how will this data be maintained and used?

Yes. The OCR 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 OCR Complaint Management System. Role-based access control (RBAC) is implemented in the OCR 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?

No. The OCR Complaint Management System does not monitor the public, GSA employees, or contractors.

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

- Ad-hoc query reports are produced on individuals
- 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? If so, what process(es) will be used to aggregate or de-identify the data?

All information in the reports is 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.

SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

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. Only relevant information to facilitate the federal sector EEO process and summary level reporting on EEO complaint activity is included in the OCR Complaint Management System.

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

Yes. GSA will create mandatory reports to Congress and to the EEOC. The data within the report is aggregate and no individual records are included.

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 or is it taken from another source? If so, what is the other source(s)?

The majority of data is collected directly from individuals, with the remaining information being related to other records or information systems, e.g. personnel files. 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.

4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?

No. 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.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

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

GSA primarily collects information directly from participants, which ensures that the information is as accurate as possible.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

Only certain OCR staff are granted access to the OCR Complaint Management System, based on their role and responsibility within OCR. 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 GSA completed a System Security Plan (SSP) for the information system(s) or application?

GSA completed the system security plans (SSPs) for the systems that support and maintain the information used for the OCR Complaint Management System. GSA categorizes all of its systems using Federal Information Processing Standard Publication 199 and Standards for Security Categorization of Federal Information and Information Systems (FIPS 199). Typically the OCR Complaint Management System is conducted on systems that are rated as "moderate

impact." Based on this categorization, GSA implements security controls from NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" to secure its systems and data. ATO was granted in November 2019. The OCR Complaint Management System is part of the EAS.

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? If so, 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 2100.1L CIO CHGE 1 GSA Information Technology Security Policy. https://www.gsa.gov/directive/gsa-information-technology-(it)-security-policy

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Individuals seeking to initiate complaints or participating in the EEO complaint process are informed that their information will be used to process their complaint. Individuals may opt out of providing information if they choose, however this may limit the facilitation of the complaint.

7.2 What procedures allow individuals to access their information?

Individuals may not access their information, as the only individuals with access to the system are OCR staff.

7.3 Can individuals amend information about themselves? If so, how?

Yes. Individuals that use the eFile system may amend their information before submitting an informal complaint. However, once the complaint is submitted, the individuals must contact OCR to amend the information from that point.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

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.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

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 OCR 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 OCR 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.

---

[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.