OCR Complaint Management System

Privacy Impact Assessment

July 8, 2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

Table of contents

SECTION 4.0 LIMITS ON USES AND SHARING OF 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?

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?

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)?

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

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

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 for the information system(s) supporting the project?

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

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline 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?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

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

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document Purpose

This document contains important details about the Office of Civil Rights (OCR) Complaint Management System. Commonly known as iComplaints, the system is a commercial off-the-shelf database used by OCR to process equal employment opportunity (EEO) cases and to generate forms and reports that are required by law to be submitted to the U.S. Equal Employment Opportunity Commission (EEOC) and Congress. OCR may, in the course of EEO case processing, collect personally identifiable information ("PII") about complainants, representatives, witnesses, responsible management officials and others who may be involved in a particular case, and manage this information in the Complaint Management System.[1]

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.[2]

System, Application or Project

OCR Complaint Management System (iComplaints). The system is described in detail in Section 1.1. below.

iComplaints includes information about**:** GSA federal employees and applicants for employment who are EEO complainants, representatives, witnesses, and potentially, GSA personnel involved in investigations.

[1] PII is any information that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

OCR maintains the following information about individuals, when relevant to EEO complaint activity, in the 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 in 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

The collection of information is mandated by EEOC regulations provided in 29 CFR parts 1614.

1.1 Why is GSA collecting the information?

The OCR Complaint Management Systems is an 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 statutes. The OCR Complaint Management System is also used to collect 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*).*

1.2 What legal authority and/or agreements allow GSA to collect the information?

29 CFR part 1614 directs federal agencies to process complaints of alleged discrimination under the laws enforced by the EEOC. EEOC Management Directive 715 *Essential Elements of Model Agency Programs under Title VII of the Civil Rights Act and Rehabilitation Act* 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/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 as set forth in EEOC regulation described in the EEOC's Management Directive 715, (MD-715) at Part B.4.a.7. https://www.eeoc.gov/federal/directives/md715.cfm

1.3 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 being collected?

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

1.4. Has any 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 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.

1.5. 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).

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

These records are collected and maintained for the purpose of counseling, investigating and adjudicating complaints of employment discrimination brought by applicants and current and former GSA employees. OCR staff is trained to handle the information they maintain in accordance with the purpose of the collection and records are partitioned within the Complaint Management System based on access needs by staff.

SECTION 2.0 OPENNESS AND TRANSPARENCY

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

2.1 Will individuals be given notice prior to the collection and/or sharing 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.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 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 direct 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.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

Yes. There is an external risk that participants may not fully understand that GSA is managing the use and implementation of the OCR Complaint Management System. To mitigate this risk, GSA identifies itself, as appropriate, in materials associated with its Complaint Management System. This includes, but is not limited to, informed consent forms, information collection instruments and training.

Internal risks exist concerning cases, especially conflict cases, being accessed by staff without a need to know. Conflict cases are considered sensitive or high-profile. OCR mitigates this by isolating conflict cases in a region within the system that can only be accessed by certain users. To further address privacy risks, OCR is in the process of reexamining all permissions and case access in the system.

SECTION 3.0 Data Minimization

GSA limits the collection of PII 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 Whose information is included in the system, application or project?

The system maintains individual data records for all individuals who contact OCR to file informal and formal EEO complaints.

The information in the OCR Complaint Management System includes information collected from complainants, witnesses, and responsible management officials that is deemed by EEO complaint processing staff as necessary for the full and proper adjudication of allegations of discrimination. In most cases these are GSA employees, however, complainants may be contractors, or applicants for employment with GSA.

3.2 What PII will the system, application or project include?

- Name
- Sexual orientation
- Prior equal employment opportunity (EEO) activity
- Age, including date of birth
- Disability, including identifying physical or mental impairments
- Grade/step/series/salary information
- Job title
- Home address
- Phone numbers
- Email addresses
- Race
- Color
- Religion
- National origin
- Gender, including transgender status
- Other identifying information deemed relevant to the investigation

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

Even without the 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 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 Form 462 Report to the EEOC more easily using the 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.

3.4 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.

3.5 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.

As previously stated, supporting documentation and evidence is stored in either locked file cabinets where only OCR staff have access and/or the secure local OCR server, which is not a part of the OCR Complaint Management System authorization boundary.

3.6 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.

3.7 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 462 report are aggregated and do not provide information on individuals

3.8 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.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

Yes, there is some risk that the system will contain information that may not be directly relevant to the filing of informal and formal EEO complaints. However, all of the records in the system receive the same level of protection.

SECTION 4.0 LIMITS ON USES AND SHARING OF 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 is included in the Complaint Management System. The data collected is maintained separately from the original sources of the information (e.g., personnel records).

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?

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 director is aware of settlement agreements and high profile cases. Management officials and witness become aware of pending investigations in which their testimony is required. The information is also shared with 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. 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, how and 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.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Once a Report of Investigation is issued to a complainant and/or to his or her attorney, the report is outside of OCR control. OCR informs all parties receiving the report that they are being provided Privacy Act-protected materials and that they must safeguard the data or risk a Privacy Act violation. The No FEAR Act Report is publicly available, so access controls in this context do not apply.

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 be verified for accuracy and completeness?

GSA primarily collects information directly from participants, which ensures that the information is as accurate as possible. In addition, when GSA partners with a third party, it outlines appropriate standards for data accuracy and completeness in its contracts.

5.2 Are there any privacy risks for individuals whose information are collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

Sensitive details of EEO complaints may become available for parties without a need to know. This may include contact information, medical documentation and disciplinary actions. Pertinent information is redacted. Complaint files are sent securely to the EEOC via electronic means. Investigation information is sent via the agency’s secure system. The reports shared externally do not request PII from individual complainants. The reports only identify general case information such as case processing timeframes and the issue(s) and basis.

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 data in the Complaint Management System, based on their role and responsibility within that office. All OCR staff who access the data have a Public Trust clearance. OCR staff will request and receive access to the system using ServiceNow. Requests require supervisor approval.

6.2 Has GSA completed a system security plan for the information system(s) or application?

Yes, GSA has completed system security plans (SSPs) for the systems that support and maintain the information used for the OCR Complaint Management System. A penetration test and assessment of controls is scheduled for June 2019. GSA categorizes all of its systems using Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199). Typically, OCR Complaint Management System is conducted on systems rated "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.

6.3 How will the system or application be secured from a physical, technological, 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 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 GSA Information Technology Security Policy. https://www.gsa.gov/directives-library/gsa-information-technology-it-security-policy-21001l-cio

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

There is always some potential risk of unauthorized use or disclosure of PII. GSA mitigates the risk of privacy incidents by providing privacy and security training to GSA personnel on the appropriate use of information and implementing breach notification processes and plans.

In addition, access is limited on a need to know basis, with logical controls limiting access to data. GSA also automates protections against overly open access controls. For example, GSA's CloudLock tool searches all GSA documents stored in Google Drive for certain keyword terms and removes the domain-wide sharing on these flagged documents until the information is reviewed. GSA agents can then review the flagged items to ensure no sensitive information has been accidentally placed in or inadvertently shared via these files.

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 are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline 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.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Yes. Regardless of whether individuals choose to participate or not, GSA may create administrative-trace data acknowledging their choice. This information describes, at minimum, a potential relationship between an individual and GSA.
GSA mitigates this risk through appropriate access controls to administrative data, by promoting transparency through this PIA, and through public comments to Information Collection Requests published in the Federal Register.

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.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

No. Privacy and security awareness training is provided to both OCR staff and all GSA employees.

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, application or project ensure that the information is used in accordance with 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 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 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.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Yes. In keeping with NIST 800-53 rev 4, control number AR-4 , GSA regularly assesses its programs to ensure effective implementation of privacy controls. While some of these assessments can be automated, such as those carried out via GSA's CloudLock tool (mentioned above), others are carried out via GSA or third-party auditors.

Auditors can pose risks because they may receive privileged access to Complaint Management System -related data, and these risks may be above and beyond those previously described.

Specifically, auditors can pose risks to: (1) confidentiality, in the form of re-identification; and (2) misuse of information. Recall that one of the ways in which GSA mitigates the normal risk of re-identification is to separately index administrative data from report data. In order to properly ensure this separation, however, GSA auditors would need access to both. Furthermore, due to their privileged access, auditors would have the ability to subject disparate datasets to shared analysis.

To mitigate this risk, GSA clearly identifies personnel with the capacity to audit its Complaint Management System program and provides employees with appropriate role-based training. Auditors perform their duties in collaboration with GSA supervisors and/or GSA’s Privacy Office.

[1] OMB Memorandum *Preparing for and Responding to a 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