United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 07/2018)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance contact your LPO.

System Name: ICOMPLAINTS	
Preparer: Renee Clark	**Office: Office of Civil Rights**
Date: 5/28/19	**Phone: 202-564-7269**
Reason for Submittal: New PIA____ Revised PIA____ Annual Review_X__ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐	
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).	

Provide a general description/overview and purpose of the system:

System contains data relative to discrimination complaints and contact information for the individuals who file them.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

This system is being implemented to be in compliance with Section 717 of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e-16; Executive Order 11748; and Section 501 of the Rehabilitation Act of 1973, as amended by Pub. L. 99-506, 100 Stat. 1807, October 21, 1986, Management Directive 110 and 715.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes the system has an SSP in XACTA. The system has been issued an ATO thru October 31, 2021.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information is not covered by the PRA.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Micropact is a FedRamp approved CSP provider providing SaaS service for the iComplaints system.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Name, Address, Date of Birth, Work address, Job Title, Office, Email address

2.2 What are the sources of the information and how is the information collected for the system?

Self-reported by individuals

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

All data in the system is self-reported. Individuals who have data in the system are notified in writing of the data that we have and are given the opportunity to update the data for accuracy. Each individual is given a point of contact to provide updated information as data such as addresses change and are advised of the importance of maintaining accurate data on file via correspondence.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

The data to be collected is of sufficient nature to put the individual at risk for identity theft if released inappropriately, informational injuries and reputational harm.

Mitigation:

The Program Office utilizes the Risk Management Framework strategy and process to comply with privacy protection requirements and minimize the privacy risk to individuals. The Agency Privacy Officer reviews all internal policies and procedures to ensure consistent application of policy, procedures and practices throughout the Agency.

OCR utilizes the Risk Management Framework strategy and process to comply with privacy protection requirements and minimize the privacy risk to individuals. ICOM monitors and audits privacy controls to ensure effective implementation. Only information absolutely necessary for the management of EEO complaints is maintained in iComplaints. Privacy information is deleted in accordance with the applicable Records Retention Schedule.

Section 3.0 Access and Data Retention by the system

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes, the system has various control levels to prevent users from accessing data outside of that necessary to perform their job function. Users are assigned system-based roles with regional access levels which allows them to access only the minimum about of data on those individuals that are within their area of the Agency.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

There is one Master Administrator who assigns each user a role which determines what type of data they can access and then assigns them areas of the Agency they can see that data for. The determination is based upon the user's job duties in the complaint process. The procedure for assigning user access is documented in the iComplaint's Administrator's Guide.

3.3 Are there other components with assigned roles and responsibilities within the system?

No

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

OCR employees at HQ's and in the Regions, members of OGC and ORC will have access to the data. Contractors will not have access to the data.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

The electronic data is retained indefinitely for the purposes of trend analysis reporting on discrimination complaints. The paper records are destroyed in accordance with EPA Records Control Schedule 0541.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Retaining the data to be collected subjects the individual to potential identity theft if inappropriately accessed, informational injuries and reputational harm.

Mitigation:

Records stored in this system are subject to EPA records schedule number (EPA 0541). System Owner of iComplaints ensures that only the needed PII elements are collected, maintained and when no longer needed are properly disposed.

The EPA Icomplaints' Administrator disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No information is shared outside of EPA as part of the normal agency operations.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None

Mitigation:

The data entered in iComplaints is not shared outside of the Agency.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

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

iComplaints' system audit logs are enabled for accountability and Intrusion Detection Systems (IDS) monitoring is enabled for the information system in real time. The PISO ensures security controls corresponding to the privacy security requirements defined in NIST Special Publication (SP) 800-53, including control enhancements are tested, reviewed, and assessed annually. The EPA iComplaint's Administrator ensures that the system remains compliant with applicable orders, policies, laws, and regulations.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

EPA personnel complete an Information Security and Privacy Awareness and General Privacy

Awareness Training course on an annual basis. The training course instructs personnel not to disseminate PII information to unauthorized individuals and how to secure information using approved techniques such as encryption. EPA's icomplaints Administrator receives notification of any employees who do not complete the annual training. Employees and contractors who do not complete the annual training have their access rights revoked until such time as they can prove completion of Security Awareness and Privacy training.

During these trainings, personnel are instructed not to release agency data classified as PII/PA//CUI to unauthorized users. An action to enforce such behavior is provided in the National Rules of Behavior. Failure to comply could result in removal of system access. Unauthorized disclosure of EPA sensitive information, including PII, may result in legal liability for the offender.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Failure to audit iComplaints and maintain an accounting of system access could potentially allow for unauthorized access to the system and a privacy breach leading to inappropriate disclosure of the PII maintained in the system resulting in informational injuries and reputational harm.

Mitigation:

iComplaints' system audit logs are enabled for accountability and Intrusion Detection Systems (IDS) monitoring is enabled for the information system in real time. The PISO ensures security controls corresponding to the privacy security requirements defined in NIST Special Publication (SP) 800-53, including control enhancements are tested, reviewed, and assessed annually. The EPA IComplaint's Administrator ensures that the system remains compliant with applicable orders, policies, laws, and regulations.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

iComplaints (ICOM) is an information management and reporting system for internal EPA use. The information collected in the ICOM system is required by 29 U.S.C. 206(d), 633a, 791 and 794a; 42 U.S.C. 2000e-16 and 2000ff-6(e), the Equal Employment Opportunity Commission (EEOC) under C.F.R. 1614.100-1614.110 and in order for the Agency to comply with EEOC Management Directive 110. Complainants provide their personally identifiable information (PII) to the EPA's Office of Civil Rights (OCR) so that they may be contacted in connection with the status of their complaint. ICOM will contain PII. Only OCR EPA staff at Headquarters and in the Regions will have access to the database via approved computers logged on thru the EPA LAN network.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X_ No___. If yes, what identifier(s) will be used.

(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

Information is retrieved by an individual's name or assigned case number.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

EPA-80

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Misuse of data maintained in the iComplaints system could be used to locate an individual's informational injuries, discrimination and reputational damage.

Mitigation:

EPA employees with a responsibility for uploading data in iComplaints limit the collection and retention of PII to only that data which is absolutely necessary for the legally authorized purpose of collection of the data. ICOM limits the collection and retention of PII to minimum elements identified. The iComplaints system owner review PII holdings and report any updates or changes to NPP. NPP updates the agency inventory and posts to the website. The agency's reporting on Privacy Management is submitted under FISMA.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Transparency mechanisms exist in the warning banners displayed prior to gaining access to iComplaints', the rules of behavior before system usage, and privacy and security notices on systems collecting data.

OCR provides notice to individuals on the formal complaint form used to collect data for input

into iComplaints.

The Privacy Act Statement (PAS) is located on the hard copy formal complaint form utilized to collect all PII from individuals for input into the iComplaints system. The PAS informs individuals of their rights to consent to the collection and sharing of PII.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

Individuals maintain the ability to access and review their PII contained in iComplaints by contacting OCR. Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g. driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Failure to provide the appropriate notice would deny individuals of their rights associated with the collection of their PII as well as loss of trust.

Mitigation:

The complaint forms used to collect PII advises everyone that they have the right to remain anonymous and not provide any PII to initiate a discrimination complaint. In instances where the individual elects to provide their PII, the initial notice is followed by correspondence to the individual advising them who to contact and how should they choose to make changes to the information provided.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals maintain the ability to access and review their PII contained in iComplaints by contacting OCR.

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g. driver's license, military identification card,

employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16."

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Each record is assigned to a case manager who has the ability to make any changes to the data within the system at the written request of the individual.

8.3 How does the system notify individuals about the procedures for correcting their information?

Individuals do not have access to the system. The system does not notify individuals about procedures for correcting their information. OCR notifies individuals in a separate letter who to contact if they feel their information is in error.

8.4 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

The physical and mental health and well-being of an individual could be damaged through breach of trust and a sense of loss of control over the use of their information.

Mitigation:

Individuals maintain the ability to access and review their PII contained in iComplaints can contact OCR at 202-564-7272.

If PII received contains errors, the individual may contact OCR to have the information corrected.

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16. "