United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

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: External Compliance Case Tracking System	
Preparer: Samuel Peterson	**Office: Office of General Counsel/External Civil Rights Compliance Office**
Date: December 5, 2019	**Phone: (202) 564-5393**
Reason for Submittal: New PIA____ Revised PIA_X___ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance X☐ 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:

The External Compliance Case Tracking System (EXCATS) was developed to allow the External Civil Rights Compliance Office (ECRCO) to manage more effectively its program information needs and to integrate all of ECRCO's various business processes, including all its compliance activities, to allow for real time access and results reporting and other varied information management needs. Among other things, EXCATS was developed to support the collection of compliance related and other identifying information needed for ECRCO to complete compliance activities and determinations.

Purpose: To support and enhance the discrimination complaint process, including the investigation and resolution of complaints, and to assure compliance with the nondiscrimination laws by recipients of federal financial assistance.

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?

Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d et seq.; Tile IX of the Education Amendments of 1972, 20 U.S.C. 1681 et seq.; Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794; Federal Water Pollution Control Act Amendments of 1972 (Pub. L. 92-500, section 13), 33 U.S.C. 1251 note; Title III of the Age Discrimination Act of 1975, 42 U.S.C. 6101 et seq.); Title VIII of the Federal Fair Housing Act (42 U.S.C. 3601); Executive Orders 11246 (Sept. 24, 1965), 12250 (Nov. 2, 1980) and 12892 (Jan. 17, 1994); 40 C. F. R Parts 5 and 7.

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?

The system security plan has been completed for the information system; the system has been issued an Authorization to Operate; the ATO expires in October 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.

There is no information collected that is covered by the Paperwork Reduction Act. No ICR is required.

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?

The data will be maintained or stored on a Cloud. The Cloud Service Provider (CSP) is FedRamp approved. The type of service that the CSP will provide is SaaS.

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).

The information the system collects include: name, contact information (address, email address, telephone number), whether the complaint is being filed on behalf of someone else, the basis for the complaint (e.g., race/color/national origin, age, religion, gender (male/female), disability, violation of the privacy of protected health information), the entity against which the complaint is being filed, when the incident(s) occurred, a brief description of what happened and the complainant's signature. In addition, several additional fields are included to assist ECRCO in processing the complaint and to provide appropriate customer service. Those fields are: an alternate person to contact if the complainant cannot be reached; whether this complaint has been filed with other agencies or is the basis of a lawsuit and, if so, to identify where else the complaint has been filed; and whether the complainant needs special accommodations for ECRCO to communicate with them (e.g. Braille, TDD). We also have included a limited number of questions to be answered to help us better assess whether we are adequately reaching and providing service to populations whose rights are covered by our statutory authorities. These questions concerning the complainant or the person on whose behalf a complaint has been filed, are: ethnicity, race, primary language spoken (if other than English), and the means by which the complainant learned about the ability to file complaints with the Office for Civil Rights. A person will be asked to provide name, address, and email address; the name and address of the person discriminated against; and the name and address of the alleged discriminating entity. Alternatively, a complainant may choose to submit a complaint in the form of a letter, or electronically. Jurisdictional Review certification process, each applicant for certification responds to ECRCO's release of confidentiality request. The questions pertain to the policies and procedures of non-discrimination; communication with persons who are limited English proficient or sensory impaired; required notices; provision of auxiliary aids to persons with sensory, manual or speech impairments; grievance procedures for disability discrimination allegations; and information regarding restrictions based on age.

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

The sources of the information collected for the system is from administrative complaints filed with EPA and related documents alleging discrimination by a recipient of EPA financial assistance and from additional information collected during the investigation phase from complainants, recipients and their employees, witnesses, EPA personnel, contractors, and from members of the public with contributory information.

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

Yes, the system uses information from commercial sources such as including census data, demographics, self-evaluation plans, analyses of workforce data. Such information is often utilized to provide comparative analysis to disparate impacts and disparate treatment allegations.

2.4 Discuss how accuracy of the data is ensured.

Data is reviewed regularly by the System Owner to assure accuracy.

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:

Since the information is collected from regular mail, electronic mail, fax, and directly from in person sources, the quality and quantity of information may differ.

Mitigation:

Each Case Manager is responsible for verifying information gathered and for ensuring that the data pertaining to his/her case is accurate.

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?

Administrative access to the records in this system is limited to ECRCO employees whose official duties require using the information. Specific access is based on need and is determined by the user's individual role in the organization. Access is managed through the use of electronic access control lists which regulate the ability to read, change and delete information in the system. System users have read-only access to designated information in the system with the ability to only modify their own submissions and those of others within their region or group. Access to confidential information is limited. The system maintains an audit trail of all actions taken in the database. All electronic data is stored on servers maintained in locked facilities with computerized access control. The server facility has appropriate environmental security controls, including measures to mitigate damage to automated information system resources caused by fire, electricity, water and inadequate climate controls. Access control to servers, individual computers and databases includes a required user log-on with a password, inactivity lockout to systems based on a specified period of time, legal notices and security warnings at log-on. The same access controls apply to remote users. System administrators have appropriate security clearances. Printed materials are filed in secure cabinets in secure federal facilities with access based on need, as described above, for the automated component of the system.

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

The MicroPact IT Operations team enforces approved authorizations for logical access to the EXCATS system. MicroPact follows the recommendations, guidance and directives of EXCATS Information Policy and recommendations/guidance provided by NIST 800-53 which provides guidance on Information System Security controls. The EXCATS application will not allow anyone other than the administrator access and permission to grant logical access to the system. The EXCATS users with Administrator privileges will create aa their user accounts and groups in compliance with their User Matrix including group account maintenance. Access control are role based and these procedures are documented in the System Security Plan at (AC-3).

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

No, other than ECRCO employees, there are no other components with assigned responsibilities the system.

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?

Administrative access to the records in this system is limited to ECRCO employees whose official duties require using the information. As MicroPact is hosting the system at a FedRamp location, under a contract that includes FAR clauses, and Privacy Act Notifications. The system maintains an audit trail of all actions taken in the database. All electronic data is stored on servers maintained in locked facilities with computerized access control. The server facility has appropriate environmental security controls, including measures to mitigate damage to automated information system resources caused by fire, electricity, water and inadequate climate controls. Access control to servers, individual computers and databases includes a required user log-on with a password, inactivity lockout to systems based on a specified period of time, legal notices and security warnings at log-on.

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.

Information is securely retained in EXCATS even when the activity, project or case is closed.

Information is destroyed after 10 years or after file closure, whichever occurs last.

The system has an EPA Records Control Schedule; the EPA Record Schedule Number is 1044.

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:

There is a risk that information could be retained longer than is required.

Mitigation:

The Records Control Schedule requires that records are to be destroyed after 10 years or after case closure whichever occurs last, the System Owner regularly monitors the EPA Records Schedule to ensure compliance.

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.

Yes, Information may be shared via EPA General Routine as delineated in the EPA System of Records Notice (SORN, EPA-21) for the EXCATS. The identity of the organizations, the information accessed and how it is to be used is also included there.

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

The uses of the records are necessary for the efficient conduct of government operations.

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?

The system does not approve information sharing agreements, MOUs, new uses of the information, and new access to the system by organizations. Access to the records in this system is limited to ECRCO employees whose official duties require using the information. Specific individualized access is structured around need and is determined by the person's role in the organization.

4.4 Does the agreement place limitations on re-dissemination?

There are no agreements regarding re-distribution in place.

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:

There is a risk that information could be shared outside of the agency for a different purpose than for the purpose that it was originally intended to be collected.

Mitigation:

ECRCO will ensure that the information is only shared consistent with EPA General Routine Uses as listed in the EXCATS SORN.

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 (Section 6.1)?

The system provides for monthly auditing and accountability conducted by the host in the form of activity logs provided to the system owner exclusively to ensure information is used for the purpose for collection.

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

ECRCO develops, implements and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

ECRCO administers basic mandatory privacy training at least annually. The training is targeted, role-based privacy training for personnel having responsibility personally identifiable information or for activities that involve PII. The name of the training is "Information Security and Privacy Awareness Training".

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Enter any content that you want to repeat, including other content controls. You can also insert this control around table rows in order to repeat parts of a table.

Privacy Risk:

None. There is no privacy risk as access to this activity record is limited to the ECRCO System Owner, exclusively. Access to information in the system is strictly limited to users who are familiar with the SORN and the PIA. The system only recognizes the users who have been authorized and provided with the individual user PIV cards that have personal passwords and additional system passwords to log in to the system.

The system tracks user log-on by password, inactivity lockout based on specified time periods, and provides legal notices and security warnings.

This activity record is available to the ECRCO System Owner at all times.

Strict Managerial oversight is observed at all times. The system only recognizes the users who have been authorized and provided with individual user PIV cards who have personal

passwords and additional system passwords to log in to the system and security training is mandatory for all users.

Mitigation:

None.

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.

To support the collection of compliance-related and other identifying information needed for ECRCO to complete compliance activities and determinations. To enhance the discrimination complaint process, including the investigation and resolution of complaints, and to ensure compliance with the nondiscrimination laws by recipients of federal financial assistance. "To collect and provide the EPA OGC/ECRCO with the ability to more effectively manage program information needs and to integrate the office's various business processes."

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, address, email address, telephone 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.)

The system is designed to collect information by name, and also to retrieve information by name.

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

The Privacy Act SORN that applies to the information is the External Civil Rights Compliance Office, External Compliance Case Tracking System (EXCATS); EPA-21

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

Access to information in the system is strictly limited to users who are familiar with the SORN and the PIA. These users have been authorized and provided with the individual user PIV cards that have personal passwords and additional system passwords to log in to the system.

Privacy Risk:

There exists a risk that should information be released consistent with the EPA General Routine Uses, the system would no longer possess the custody over it to ensure that privacy would be maintained.

Mitigation:

User under the general routine use are guided by law which prevent unauthorized use of the information they have received.

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.

Individuals who are required to provide information are informed via the ECRCO Privacy Act Statement Routine Use Statement which states in part:

"This information may be disclosed to a Federal, State, or local agency where necessary to enable ECRCO to investigate and resolve discrimination complaints and ensure compliance with non-discrimination laws by recipients of EPA financial assistance. Additionally, this information may be disclosed consistent with the Routine Uses to commercial collection agencies under contract with the EPA, as provided by 31 U.S.C. 3718 and 40 CFR part 13, for collection Purposes or pursuant to the Routine Uses outlined in EXCATS System of Records Notice, related to and compatible with the original purpose for which the information was collected."

Individuals seeking to file a complaint with ECRCO are also informed that the information that they are providing is voluntary and that the disclosure of that information is governed by the Privacy Act. Individuals are informed that the failure to provide this information may prevent the ECRCO from investigating their complaint.

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 are informed that the information provided is voluntary and necessary for investigating their complaint. Individuals are not provided opportunities to opt out of the sharing of information determined to be essential for the continued administration of their cases.

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:

Low risk. There is a possibility that individual may not fully understand the uses of their information prior to signing the privacy notice.

Mitigation:

Adequate information is provided to user in plain language to understand how their information will be used prior to signing the privacy notice.

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 seeking access to their own personal information in this system of records will be 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 regulation 40 CFR part 16.

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

Any individual who wants to contest or correct the contents of a record, should submit a written request to the EPA, Attn: Agency Privacy Officer, WJC West, MC2831T, 1200 Pennsylvania Avenue, NW., Washington, DC 20460, privacy@epa.gov.

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

Any individual who wants to correct the contents of a record, is informed to submit a written request to the EPA, Attn: Agency Privacy Officer, WJC West, MC2831T, 1200 Pennsylvania Avenue, NW., Washington, DC 20460, privacy@epa.gov.

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:

Low risk. Information collected in the system is continually held in a closed system and is not available to the public.

Mitigation:

As soon as the EXCATS System is made aware of the existence of incorrect information and for the necessity to correct it, that correction is effectuated immediately.