United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: Equal Employment Opportunity Case Management **(EECOM)**		**System Owner:** JuanCarlos Hunt	
Preparer: Kwasi Griffin		**Office:** Office of Civil Rights & Adjudication OA-OCRA	
Date: 03/11/2026		**Phone:** 202-564-8153	
Reason for Submittal:			
New: ☐	Revised: ☐	Annual Review: ☒	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☒	
Operation & Maintenance: ☒	Rescindment/Decommission: ☐		

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:

In pursuing its mission, Office of Civil Rights and Adjudication (OCRA) uses a networked infrastructure related to discrimination complaints and contact information for the individuals who file them, and processing needs to employees, contractors, and partners. This system is designed to allow for the processing and storage of Equal Employment Opportunity (EEOCM) complaints filed by EPA employees.

Section 1. 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 was 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. SORN:EPA-80,[FRL-9995-21-OMS].

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 has an updated and approved System Security Plan and has been issued continuous Authorization to Operate (ATO) by the Authorization Official (AO).

The memo was signed 10/30/2025. The ATO expires 6/1/2026.

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?

Tyler Federal LLC is a FedRamp approved CSP provider providing SaaS service for the EEOCM system.

Section 2. 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?

The information collected is typically provided by the individual or employee. In cases where information is not obtained from the individual or employee, the Agency collects such information in accordance with applicable laws and pursuant to applicable agreements governing the sharing of such information (e.g. Memoranda of Understanding, Memoranda of Agreement)

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 EEOCM does not use information from outside sources. It's not a database that uses data from another source, and it's not an application which would reference any external information. Its only purpose is to host/store Agency 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 is advised of the importance of maintaining accurate data on file via correspondence.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

The EEOCM does not use information from outside sources. It's not a database that uses data from another source, and it's not an application which would reference any external information. Its only purpose is to host/store Agency data.

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.

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

Section 3. 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 systems employ strict access control mechanisms designed to enforce the privilege principle. Only users with a legitimate business need are granted access to sensitive information. As a result, unauthorized users are prevented from viewing, editing, or otherwise interacting with information

outside their purview. This reduces the risk of data breaches and helps maintain confidentiality and compliance with data protection regulations.
The implementation of access control levels ensures that users only access information necessary for their duties, thereby supporting data security and compliance objectives.
To further mitigate risks, access controls are reviewed regularly and updated as roles or responsibilities change. Additionally, audit logs are maintained to monitor access and identify any unauthorized attempts, allowing prompt response to potential security incidents.

.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

The access control levels are documented in the System Security Plan (SSP), User's Guide, and Standing Operating Procedures.

Role-Based Access Controls are in place to ensure that information is accessed in accordance with the uses described above. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Users of the information system are only given controls to access the information that is essential and pertinent to complete their duty assignments. This is accomplished through strict adherence to EPA CIO Policy CIO 2150-P-01.4 "INFORMATION SECURITY – ACCESS CONTROL PROCEDURE", as well as, technically enforced with implementation of Defense Information Systems Agency (DISA) Security Technical Implementation Guides related to NIST control AC-6 "Least Privilege." Additionally, the PIA and SORN are clear about the uses of information under "routine use". The information contained in the system is relevant to the mission of the EPA. Any violations of access or use of the information are investigated by the Privacy Officer and ISO and referred to the supervisor and human resources for disciplinary action.

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?

An individual is assigned the type of access they need to complete their duty tasks. The supervisor maintains a functional category form on employees that is reviewed annually. Monitors and audits are completed on the functional categories by the supervisor and ISO. Contractors don't have access to the computer system. They are required to complete annual Privacy, Security, and Rules of Behavior training. The Privacy Officer and ISO monitor that the annual Privacy, Security, and Rules of Behavior training are completed by contractors and business associates.

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 EEOCM ensures that only the PII elements needed are collected, maintained and when no longer needed are properly disposed.

The EPA EEOCM' 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. 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 governments, 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.

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 external sharing is compatible with the original purposes of the collection.

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

EPA policy requires that any connections from the information system to other information systems must be documented in an Interconnection Security Agreements (ISA). For connecting systems that have the same Senior Information Official (SIO), an ISA is not required. Rather, the interface characteristics between the connecting information systems shall be described in the System Security Plans (SSP) for the respective systems. Any ISA or Memorandum of Understanding / Agreement (MOU/A) must be reviewed, approved, and signed by the SIO. MOUs are reviewed by Local Privacy Officer and the Agency Privacy Officer following internal procedures prior to issuing.

4.4 Does the agreement place limitations on re-dissemination?

Currently there are no shared agreements 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:
None.

Mitigation:

The data entered into EEOCM is not shared outside of the Agency.

Section 5. 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 as stated in Section 6.1?

EEOCM' 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 EEOCM'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 EEOCM 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

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

Failure to audit EEOCM 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:

EEOCM' 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 EEOCM's Administrator ensures that the system remains compliant with applicable orders, policies, laws, and regulations.

Section 6. 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

EEOCM is an information management and reporting system for internal EPA use. The information collected in the EEOCM 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 and Adjudication (OCRA) so that they may be contacted in connection with the status of their complaint. ICOM will contain PII. Only OCRA 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: ☒ 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 type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.)

The Agency minimizes this risk by enforcing access controls to minimize the number of individuals who have access to the data and by storing data on systems that have been accredited as

secure for this type of data. Staff are also trained in how to handle potential breaches to minimize negative impacts. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Users of the information system are only given controls to access the information that is essential and pertinent to complete their duty assignments. This is accomplished through strict adherence to EPA CIO Policy CIO 2150-P-01.4 "INFORMATION SECURITY – ACCESS CONTROL PROCEDURE", as well as, technically enforced with implementation of Defense Information Systems Agency (DISA) Security Technical Implementation Guides related to NIST control AC-6 "Least Privilege." Additionally, the PIA and SORN are clear about the uses of information under "routine use". The information contained in the system is relevant to the mission of the EPA. Any violations of access or use of the information are investigated by the Privacy Officer and ISO and referred to the supervisor and human resources for disciplinary action.

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 EEOCM system could be used to locate an individual's informational injuries, discrimination and reputational damage. There is a risk for unauthorized access and misuse of data elements in the system.

Mitigation:

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

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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 EEOCM, 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 EEOCM The Privacy Act Statement (PAS) is located on the hard copy formal complaint formed to collect all PII from individuals for input into the EEOCM system. The PAS informs individuals of their rights to consent to the collection and sharing of PII.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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 EEOCM by contacting OCRA. 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 advise 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 with the individual advising them who to contact and how they should choose to make changes to the information provided.

Section 8. 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 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?

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.

8.3 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 Freedom of Information Act (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 who maintain the ability to access and review their PII contained in EEOCM can contact OCRA at 202-564-0092.

If PII contains errors, the individual may contact OCRA 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. "

I attest as the Agency Privacy Officer that **Equal Employment Case Management (EEOCM)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.04.28 15:00:33 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA