U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: icomplaints
Bureau/Office: Office of the Secretary
Date: September 29, 2017
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

icomplaints is a Departmental Web-based system for enterprise-wide management of Equal Employment Opportunity (EEO) complaints. icomplaints is used to track and monitor discrimination complaints, as well as identify trends in discrimination complaints throughout the Department, allowing the Departmental Office of Civil Rights and Bureau EEO Offices to implement preventive measures to eliminate workplace discrimination, and reduce the number of complaints filed throughout the Department. icomplaints users utilize the system to process EEO complaints at all stages of the

complaints process, to assist with timely processing of complaints as required by the Equal Employment Opportunity Commission (EEOC), to monitor potential patterns of discrimination, and to reports within the Department, to the EEOC, and to Congress, including the Annual Federal EEO Statistical Report of discrimination complaints and the quarterly and annual No Fear Act Reports, as required by Congress. Icomplaints is a cloud based system hosted by Micropact Inc.

C. What is the legal authority?

Title VI and Title VII of the Civil Rights Act of 1964, as amended (42 U.S.C. 2000d and 42 U.S.C. 2000e, et seq); Section 501, Section 504 and Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 791, et seq) and its implementing regulations; the Age Discrimination in Employment Act of 1967, as amended (29 U.S.C. 794, et seq) and its implementing regulations; the Age Discrimination in Employment Act of 1967, as amended (29 U.S.C. 621, et seq); Title IX of the Education Amendments of 1972 (Pub. L. 92-318); Section 403 of the Trans-Alaska Pipeline Authorization Act (Pub. L. 93-153.87 Stat. 576); the Americans with Disabilities Act of 1990 (Pub. L. 101-336); the Age Discrimination Act of 1975 (29 U.S.C. 621); the Architectural Barriers Act of 1968 (Pub. L. 90-480); the Civil Rights Restoration Act of 1987 (Pub. L. 100-259); the Civil Rights Act of 1991 (Pub. L. 102-166); the Health Insurance Portability and Accountability Act of 1196 (Pub. L. 104-191); and Department of the Interior Regulations at 43 CFR Parts 17 and 41; Presidential Executive Orders 12898, 13160, 13166, 13152 and 13145; 373 DM 8, dated July 1, 2005, and 373 DM 7, dated December 1, 1998.

EEOC Regulation 29 C.F.R. §1614.602(a) requires agencies to report to the EEOC information concerning pre-complaint counseling and the status, processing and disposition of complaints under this part at such times and in such manner as the Commission prescribes. The requirement to file an EEOC Form 462 Report applies to all federal agencies and departments covered by 29 C.F.R. Part 1614, as defined in 29 C.F.R. § 1614.103(b). This includes Executive agencies as defined in 5 U.S.C. 105, Military departments as defined in 5 U.S.C. 102, the Government Printing Office, the Postal Regulatory Commission, the Smithsonian Institution, the Tennessee Valley Authority, the United States Postal Service, and those units of the judicial branch of the federal government having positions in the competitive service. The EEOC also recommends that Agencies use comprehensive complaints tracking systems and continually take steps to ensure that the system is updated with the most current information at each stage of the EEO process.

D. Why is this PIA being completed or modified?

☐New Information System
☐New Electronic Collection
☒Existing Information System under Periodic Review
☐Merging of Systems
☐Significantly Modified Information System
☐Conversion from Paper to Electronic Records
☐Retiring or Decommissioning a System

☐Other: *Describe*

E. Is this information system registered in CSAM?

☒Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-000000661
SSP Name: icomplaints System Security Plan

☐No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒Yes: *List Privacy Act SORN Identifier(s)*

Records are maintained under government-wide system of records notice EEOC/GOVT-1, Equal Employment Opportunity (EEO) in the Federal Government Complaint and Appeal Records (81 FR 81135, November 17, 2016), and DOI-18, Civil Rights Complaints and Compliance Review Files, system of records notice (73 FR 19088, April 8, 2008), which supplements EEOC/GOVT-1. These SORNs may be viewed on the DOI SORN website at: https://www.doi.gov/privacy/sorn.

The DOI-18 SORN is being modified to provide general and administrative updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

☐No

H. Does this information system or electronic collection require an OMB Control Number?

☐Yes: *Describe*
☒No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒Name
☒Gender
☒Birth Date
☒Religious Preference
☒Medical Information
☒Disability Information
☒Race/Ethnicity
☒Personal Cell Telephone Number
☒Personal Email Address
☒Home Telephone Number
☒Employment Information
☒Mailing/Home Address
☒Other: *Specify the PII collected.*

Unique Identification Number (UID), National Origin, and Sexual Orientation/Gender Identity. The PII collected varies for each case depending on the particular claims or bases alleged by the complainant. Whether or not an individual's personal email, cell, or home telephone number is provided depends on what information a complainant or witnesses chooses to provide as their contact information. In addition, PII may be obtained pertaining to similarly situated individuals to compare their treatment to Complainant in order to allow the adjudicator to determine whether or not discrimination has occurred. This information is included in a Report of Investigation (ROI), which is uploaded into icomplaints.

B. What is the source for the PII collected? Indicate all that apply.

☒Individual
☐Federal agency
☐Tribal agency
☐Local agency
☒DOI records
☐Third party source
☐State agency
☒Other: *Describe*

The source of PII collected is dependent on the particular allegation of discrimination in a given complaint. If a complainant is alleging discrimination pertaining to a personnel action (e.g. a selection, promotion, suspension, termination, etc.) then information is typically obtained from Human Resources (HR) officials pertaining to the personnel action as part of the EEO investigation into the complaint. If requested by the EEO Investigator, an SF-50 may be obtained from HR for inclusion in the Report of Investigation. For each complaint, an EEO Investigator typically submits a request for information

through the Bureau EEO Office or Office of the Secretary EEO Office, who then works with HR and other agency officials as necessary to obtain the requested information, including any documents requested. The source of the information is typically provided as part of the response to the request for information. Once an EEO investigation concludes, the Report of Investigation is issued to the complainant, and a copy of the Report of Investigation is also uploaded into icomplaints.

C. How will the information be collected? Indicate all that apply.

☒Paper Format
☒Email
☒Face-to-Face Contact
☐Website
☒Fax
☒Telephone Interview
☐Information Shared Between Systems
☐Other: *Describe*

D. What is the intended use of the PII collected?

The intended use of the PII that may be collected for a given complaint is to provide sufficient information to a fact finder during the adjudication of the complaint to determine whether or not discrimination has occurred. PII pertaining to a complainant's or witness' contact information is used to contact the complainant or witness throughout the course of the processing and adjudication of the complaint. The complainant's first and last name is utilized in icomplaints as a way of identifying the complaint and assigning a system generated case number.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Bureau/office EEO practitioners, Counselors, and EEO Officers use the PII that may be uploaded into icomplaints or included in icomplaints to process complaints of discrimination filed by DOI employees, former employees or applicants for employment.

☒Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

DOI attorneys who are assigned to defend the agency in complaints of discrimination that go before an EEOC Administrative Judge for hearing are provided the Report of Investigation (ROI) which is maintained in the system for each complaint to which they are assigned. The ROI contains PII. Each ROI has a Privacy Act Statement. The SOL attorneys do not have access to the icomplaints system.

☒Other Federal Agencies: *Describe the federal agency and how the data will be used.*

In a Mixed Case complaint or Mixed Case appeal, the Merit Systems Protection Board (MSPB) assigned would have access to the ROI in hard copy format. In addition, Reports of Investigation for complaints of discrimination that go before an EEOC Administrative Judge for hearing and complaint files for appellate cases pending before the EEOC are uploaded into the EEOC's Federal Sector EEO Portal (FedSEP) is the Commission's online data system that allows agencies to submit their affirmative employment plans (MD-715 report), complaint processing data (Form 462), and complaint files for hearings and appellate cases (Hearings and Appeals). In addition, FedSEP will offer agencies the opportunity to communicate with the Commission as well as other agencies. At the present time, FedSEP offers: (1) MD-715 data collection; and (2) Form 462 data collection.

Only in instances where there is a conflict of interest, will a case be transferred to another Federal Agency until closure of case. Other federal agencies are under the same IT Security and Privacy Act compliance regulations as the DOI.

Information may be shared with other Federal agencies other Federal agencies charged with the enforcement of equal employment opportunity laws, orders and regulations, on a need-to-know basis to assist these agencies in their enforcement activities; and for other authorized purposes as outlined in the routines uses in the DOI-18 system of records notice.

☐Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒Contractor: *Describe the contractor and how the data will be used.*

For Conflict of Interest cases, a contractor or another agency would be involved. Contractors may in addition provide the OCR office assistance with Final Agency Decision (FAD) writing when the caseload of the internal FAD writers is heavy. Contractors do not have access to icomplaints; however, some ROI's will include some PII for the purposes of comparing data pertaining to the protected EEO categories of the Complainant and other similarly situated individuals to allow an adjudicator to determine whether or not discrimination occurred.

☐Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Any individual may decline to provide information needed to process discrimination complaints. If an individual declines to provide requested information, his/her complaint may not be processed. Individuals sign a consent form when they decline to provide information.

☐No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒Privacy Act Statement: *Describe each applicable format.*

Individuals are provided notice through a Privacy Act Statement contained on the DI-1892, Complaint of Discrimination Form, which is completed by the individual during the initial stages of the complaint process.

☒Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment and the published DOI-18, Civil Rights Complaints and Compliance Review Files system of records notice.

☐Other: *Describe each applicable format.*

☐None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data will be retrieved by various fields including name of complainant, Bureau unique Identifier, date of request, Bureau/Office location, type of employee, agency complaint number, and the organizational affiliation of the complainant. Data is retrieved both manually for special requests and via reports generated automatically.

I. Will reports be produced on individuals?

☒Yes: *What will be the use of these reports? Who will have access to them?*

The system produces reports using various parameters determined by users but is limited to only the information that has been approved by the complainants or contained in the complainant's case files. The reports will enable the icomplaints headquarters and bureau EEO specialists/administrators to determine certain information regarding complaints submitted including types of complaints, categories of complaints, and number of complaints. The profile of information will only be provided to the users of icomplaints. Security measures are enforced to control which users have access to areas of aggregated information that is used to prepare The EEOC Form 462 Report, The No Fear Act Report, and special reports to analyze trends and patterns regarding discrimination complaints throughout the department.

☐No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Not applicable. We do not have any other sources other than the icomplaints systems and its processes. The system is monitored by the OCR icomplaints staff for accuracy of data input.

B. How will data be checked for completeness?

Users are required to provide complete information in the system. If information is not complete, error messages are provided by the system before moving onto the next screen. Business Rules for each of the icomplaints Events can be enabled to increase accuracy of data that users input into the icomplaints system. Error messages notify the system user that information is required prior to moving onto the next field item. Also, the system is monitored by the OCR icomplaints staff for accuracy of data input.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Information is obtained from each complainant and from documents contained in each case file, including EEO Counselor's Reports, Reports of Investigation, and documents developed by the Office of Civil Rights. The Office of Civil Rights icomplaints staff monitors the accuracy of the data in the icomplaints system to ensure that the data is current.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

icomplaints records adhere to General Records Schedule (GRS) 2.3, which was approved by the National Archives and Records Administration (NARA). GRS 2.3 covers EEO records, with different retention periods based on type of records as follows:

Item 31, EEO official discrimination complaint case files – Informal process (DAA-GRS- 2015-0007-0007). The records disposition is temporary. Records are destroyed 3 years after resolution of case, but longer retention is authorized if required for business use.

Item 32, EEO official discrimination complaint case files – Formal process (DAA-GRS- 2015-0007-0008). The records disposition is temporary. Records are destroyed 7 years after resolution of case, but longer retention is authorized if required for business use.

Item 033, EEO case files that did not result in an EEO complaint (DAA-GRS- 2015-0007- 0009). This includes cases that did not result in an official formal or informal EEO complaint. The records

disposition is temporary. Records are destroyed 2 years after final resolution of case, but longer retention is authorized if required for business use.

Item 034, EEO compliance review files (DAA-GRS- 2015-0007- 0010). This includes reviews, background documents, and correspondence relating to contractor employment practices. The records disposition is temporary. Records are destroyed when 7 years old, but longer retention is authorized if required for business use.

035 EEO reports and employment statistics files (DAA-GRS- 2015-0007- 0011). This includes the annual report to the EEOC, the annual report to Congress on the No FEAR Act, quarterly/monthly reports to senior leadership, and other related reports required by EEOC's MD 715 (such as the Analysis and Action Plans) or succeeding guidance as well as employment statistics files which support reporting requirements to Congress, the EEOC and other oversight entities. The records disposition is temporary. Records are destroyed when 5 years old, but longer retention is authorized if required for business use.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

When approved for destruction, paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with NARA guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to individual privacy for use of icomplaints due to the sensitive PII and content related to individual complaints of discrimination. Through the use of continuous monitoring measures including the use and completion of the OCR User Access From that is submitted to the OCR Administrator(s), prior to a user gaining access to the system. A user account is approved to be created after completion of the above mentioned form. User account(s) are immediately deactivated after a user leaves a bureau or office in the DOI. Audit logs are regularly reviewed in order to determine whether a user account has been inactive for a long period of time. If that is the case, a user account is deactivated and a new user access form must be submitted if a user wants to gain access into the system after log activity shows no access by the user in a long period of time. Furthermore, if a case that is a conflict of interest case is being transferred to another Federal agency, the federal agency that inherited the conflict case is under the same IT security and privacy act rules and regulations as the DOI so risk is moderate. Outside agencies do not have access to the DOI icomplaints system. Additional security measures are pursuant to OMB Circulars A-123, and A-130, NIST SP 800-53, Revision 4, DOI IT Security and Privacy Control standards, and FedRAMP Continuous Monitoring procedures, the icomplaints tracking system has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: review of audit log activity; DOI Privacy Act warning notice banner; verification of trusted security certificates from Micropact's site; password and user identification;

database permissions; determination of user(s) role and location permissions provided independently and according to a user(s) role in the intake process; and other application end controls.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒Yes: *Explanation*

The information collected in icomplaints is necessary, and directly related to the reason for which the system has been designed. The majority of the data elements are required for preparation, submission, and processing of EEO complaints, reports for the EEOC, and other annual reports to Congress.

☐No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒No

C. Will the new data be placed in the individual's record?

☐Yes: *Explanation*
☒No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐Yes: *Explanation*
☒No

E. How will the new data be verified for relevance and accuracy?

New data is not being created.

F. Are the data or the processes being consolidated?

☐Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒No, data or processes are not being consolidated.

icomplaints is designed to protect data fields once the EEO complaint data has been entered and completed. Access and permission levels have been established by the DOI OCR and authorized only to those persons who must have the information contained in the system in order to carry out their duties. Pursuant to OMB Circulars A-123, and A-130, the electronic icomplaints tracking system has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: audit logs, DOI Privacy Act warning notice banner, verification of trusted security certificates from Micropact's site, passwords and user identification, database permissions, roles, location permissions, and application controls.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒Users
☒Contractors
☒Developers
☒System Administrator
☒Other: *Describe*

Users of the system will include the following EEO Practitioners: EEO Counselors, EEO Specialists and the OCR System Managers and Staff, and the Micropact Contractors in order to carry out their official duties.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access is based on a user profile provided on their User Access Forms submitted to the OCR System Administrators, and role privileges authorized by the user's supervisor and the DOI system manager. Electronic data is protected through user identification, passwords, thirty (30) day password expiration enforcement, database permissions and role, location and Bureau based controls. Such security measures establish different access levels for different types of users. In other words, users only have access to data when approved.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Yes. Contractors are involved with the design and development of the system, and maintenance and updates to the system at the server level. A Privacy Act clause was included as part of the statement of work and the contractor was provided with copies of the Department of Interior's Privacy Act and applicable policies.

☐No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐Yes. *Explanation*
☒No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐Yes. *Explanation*

☒No - The system is not designed to monitor individuals. It does not monitor complainants. It monitors the system administrators (EEO Specialists that work in the icomplaints system).

L. What kinds of information are collected as a function of the monitoring of individuals?

icomplaints is not designed to monitor individuals, so there is no monitoring. However, icomplaints administrators use audit logs to prevent unauthorised use and user behaviors. Through this auditing process, usernames, IP addresses, and time/date and login status are gathered to support incident response and troubleshooting.

M. What controls will be used to prevent unauthorized monitoring?

icomplaints is designed to protect data fields once the EEO complaint data has been entered and completed. Access and permission levels have been established by the DOI OCR and authorized only to those persons who must have the information contained in the system in order to carry out their duties. Pursuant to 0MB Circulars A-123, and A-130, the electronic icomplaints tracking system has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: audit logs, DOI Privacy Act warning notice banner, verification of trusted security certificates from Micropact's site, strong password and user authentication, database permissions, roles, and access controls, permissions and other application controls.

No user can access the icomplaints system without prior approval from the System Manager of the icomplaints system. There is a process that is set in place in order for a Bureau EEO Practitioner to obtain access into the icomplaints system by the completion of an OCR System Access Form and other requirements that are requested and required prior to an EEO Practitioner from a Bureau gaining access into the icomplaints system. The OCR follows the DOI and other Federal Government IT Security Standards for this system.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒Security Guards
☐Key Guards
☐Locked File Cabinets
☒Secured Facility
☒Closed Circuit Television
☐Cipher Locks
☒Identification Badges
☐Safes
☒Combination Locks
☒Locked Offices
☒Other. *Describe*

The Micropact data center has 24/7 guards.

(2) Technical Controls. Indicate all that apply.

☒Password
☒Firewall
☒Encryption
☒User Identification
☐Biometrics
☒Intrusion Detection System (IDS)
☒Virtual Private Network (VPN)
☒Public Key Infrastructure (PKI) Certificates
☒Personal Identity Verification (PIV) Card
☐Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒Periodic Security Audits
☒Backups Secured Off-site
☒Rules of Behavior

☒Role-Based Training
☒Regular Monitoring of Users' Security Practices
☒Methods to Ensure Only Authorized Personnel Have Access to PII
☒Encryption of Backups Containing Sensitive Data
☒Mandatory Security, Privacy and Records Management Training
☐Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The officials responsible for protecting the privacy for the use of this system is the icomplaints Information System Owner, Privacy Act System Manager, Information System Security Officer (ISSO), the DOI EEO Practitioners/Specialists who are authorized users working on cases in the system, EEO Investigators, and the Micropact Contractors who use this system to carry out their official duties to provide services and host this system in their cloud based facility.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The icomplaints Information System Owner, Privacy Act System Manager, and the Information System Security Officer (ISSO), are responsible for establishing policy, controls and safeguards to protect privacy and security for icomplaints in accordance with Federal laws and policy. EEO officers, staff members and agency advisors are responsible for assuring proper use of the data. The System Owner, ISSO, Privacy Act System Manager, and all authorized users are responsible for immediately reporting any potential or suspected compromise or breach of PII to DOI-CIRC, the Department's incident reporting portal, in accordance with Federal policy and established DOI policy and procedures.