Management Bureau/Chief Information Officer/Information Assurance
(M/CIO/IA)

PRIVACY IMPACT ASSESSMENT (PIA)

USAID Equal Employment Opportunity (EEO) Program

iComplaints

Approved: June 24, 2014

TABLE OF CONTENTS

1. INTRODUCTION

The USAID Privacy Office is using this Privacy Impact Assessment (PIA) Template to gather information from program managers, system owners, and information system security officers in order to analyze USAID information technology and information collections (systems) that collect, use, maintain, or disseminate personally identifiable information (PII).

The PIA process should accomplish two goals: 1) determine the privacy risks and effects of collecting, using, maintaining, and disseminating PII; and 2) evaluate and enforce protections and alternative processes for handling PII to reduce potential privacy risks to acceptable levels.

Type *Not Applicable* in the answer boxes for those questions that do not apply to your system and explain why the question is not applicable. Each section includes assistance (in blue text) on how to answer the question. For additional instructions on how to complete this PIA Template, please see Appendix C Conducting the PIA.

If you have questions about or would like assistance with this PIA Template, the PIA process, or other privacy compliance requirements please contact the USAID Privacy Office at privacy@usaid.gov.

2. INFORMATION

2.1 PROGRAM INFORMATION

2.1.1 Describe the program and its purpose.

The Office of Civil Rights and Diversity (OCRD) administers USAID's equal employment opportunity (EEO) programs, including the development and implementation of EEO policy. OCRD works with employees and management to ensure that the USAID workplace is free from discrimination and harassment.

OCRD's mission is to promote EEO, respect, diversity, and inclusion across USAID to comply with federal and Agency policies of EEO and diversity. OCRD's mission is grounded in USAID's core values and USAID Forward priorities and reflects the commitment to provide its workforce with a supportive environment in which each person feels empowered to achieve his or her full potential.

Currently, OCRD is working in the following areas:

- Dispute Resolution
- Outreach and Training
- Diversity and Inclusion Initiatives
- Anti-Harassment Program
- Reasonable Accommodation

2.1.2 What types of paper documents, systems, electronic media, digital collaboration tools or services, and/or mobile services do you employ to collect, use, maintain, and disseminate information?

OCRD collects, uses, maintains, and disseminates information in a variety of ways. OCRD uses iComplaints, an automated tracking system that provides information on the status of EEO cases from the pre-complaint stage through the formal decision process.

OCRD produces paper copies and maintains hard copy files of all documents in secured filing cabinets, as well as electronic copy files in the OCRD P: drive, at all stages of the EEO complaint and ADR process.

Last, upon request from the EEOC, OCRD provides full administrative files, including all forms and documentation, to the EEOC via secure connection at https://efx.eeoc.gov/usa.

2.1.3 How do you retrieve information?

Information on complaints is retrieved by searching the name of the aggrieved or complainant the following ways:

1. Different types of electronic search functions using iComplaints;
2. Hard copy forms filed in a secure filing cabinet;
3. Electronic copy forms in the OCRD P: drive.

2.2 INFORMATION COLLECTION, USE, MAINTENANCE, AND DISSEMINATION

2.2.1 What types of personally identifiable information (PII) do you collect, use, maintain, or disseminate?

(Please check all that apply. If you choose Other, *please list the additional types of PII.)*

☒ Name, Former Name, or Alias

☐ Mother’s Maiden Name

☐ Social Security Number or Truncated SSN

☒ Date of Birth

☒ Place of Birth

☒ Home Address

☒ Home Phone Number

☒ Personal Cell Phone Number

☒ Personal E-Mail Address

☒ Work Phone Number

☒ Work E-Mail Address

☐ Driver’s License Number

☐ Passport Number or Green Card Number

☐ Employee Number or Other Employee Identifier

☐ Tax Identification Number

☐ Credit Card Number or Other Financial Account Number

☐ Patient Identification Number

☐ Employment or Salary Record

☒ Medical Record

2.2.1 What types of personally identifiable information (PII) do you collect, use, maintain, or disseminate?

(Please check all that apply. If you choose Other, *please list the additional types of PII.)*

☐ Criminal Record

☐ Military Record

☐ Financial Record

☒ Education Record

☐ Biometric Record (signature, fingerprint, photograph, voice print, physical movement, DNA marker, retinal scan, etc.)

☒ Sex or Gender

☒ Age

☐ Other Physical Characteristic (eye color, hair color, height, tattoo)

☒ Sexual Orientation

☒ Marital status or Family Information

☒ Race or Ethnicity

☒ Religion

☒ Citizenship

☒ Other: Additional PII that is voluntarily provided by the complainants and others submitting pertinent information and OCRD collects documents, such as emails, related to the complainant that might contain PII.

☐ None

2.2.2 About whom do you collect personal information?

(Please check all that apply. If you choose Other, *please provide the types of people.)*

☒ Citizens of the United States

☒ Aliens lawfully admitted to the United States for permanent residence

☒ USAID employees, including Foreign Service National (FSN) Direct Hires, FSN Personal Services Contractors, and Third Country National Employees (non-US citizens for informal EEO process only)

☒ Employees of USAID contractors or service providers (for informal EEO process only)

☐ Visitors to the United States

☒ Aliens

☐ Business Owners or Executives

☐ Others:

2.2.3 What types of device, website, or platform related data associated with digital or mobile programs or services do you collect, use, maintain, or disseminate?

(Please check all that apply. If you choose Other, *please provide the types of data.)*

☐ Log Data (IP address, time, date, referrer site, browser type)

☐ Tracking Data (single- or multi-session cookies, beacons)

☐ Form Data

☐ User Names

☐ Passwords

☐ Unique Device Identifier

☐ Location or GPS Data

☐ Camera Controls (photo, video, videoconference)

☐ Microphone Controls

☐ Other Hardware or Software Controls

☐ Photo Data

☐ Audio or Sound Data

☐ Other Device Sensor Controls or Data

☐ On/Off Status and Controls

☐ Cell Tower Records (logs, user location, time, date)

2.2.3 What types of device, website, or platform related data associated with digital or mobile programs or services do you collect, use, maintain, or disseminate?

(Please check all that apply. If you choose Other, *please provide the types of data.)*

☐ Data Collected by Apps (itemize)

☐ Contact List and Directories

☐ Biometric Data or Related Data

☐ SD Card or Other Stored Data

☐ Network Status

☐ Network Communications Data

☐ Device Settings or Preferences (security, sharing, status)

☐ Other:

☐ None

2.2.4 What PII, digital data, or mobile data *could be* made available to USAID or its contractors and service providers?

In addition to collecting PII in the EEO complaint process, additional PII might be provided voluntarily by the aggrieved or complainant and other persons submitting information.

2.2.5 What are the authorities that permit you to collect, use, maintain, or disseminate PII and, specifically, Social Security Numbers (SSNs)?

Pub. L. 110–233, 122 Stat. 881; 5 U.S.C. 2301 note (Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act)); 29 U.S.C. 206(d); 29 U.S.C. 633a; 29 U.S.C. 791; 42 U.S.C. 2000e–16; E.O. 11478 34 FR 12985, 3 CFR, 1966-1970 Comp., p. 803, as amended; 29 CFR 1608 and 1614; EEOC Management Directive MD-110.

2.2.6 Who owns and/or controls the PII?

(Please check all that apply. Please provide the names of the specific organizations. If you choose Other, *please provide the types of organizations and the name of each organization.)*

☒ USAID Office: Office of Civil Rights and Diversity (OCRD) owns the PII and controls access to the PII by USAID employees.

☐ Another Federal Agency:

☒ Contractor: MicroPact, Inc., 12901 Worldgate Drive, Suite 800, Herndon, VA 20170-6014, controls access to the PII by MicroPact administrators.

2.2.6 Who owns and/or controls the PII?

(Please check all that apply. Please provide the names of the specific organizations. If you choose Other, *please provide the types of organizations and the name of each organization.)*

☐ Cloud Computing Services Provider:

☐ Third-Party Web Services Provider:

☐ Mobile Services Provider:

☐ Digital Collaboration Tools or Services Provider:

☐ Other:

AR-3 Privacy Requirements for Contractors and Service Providers
UL-1 Internal Use

2.2.7 Who has access to the PII at USAID?

OCRD staffs that have need-to-know and MicroPact administrators who manage the system have access to the PII in iComplaints.

2.2.8 With whom do you share the PII outside of USAID?

OCRD tracks and reports to the U.S. Equal Employment Opportunity Commission (EEOC) all USAID EEO activities pursuant to 29 CFR 1614. The reports to the EEOC are comprised of numerical data, as well as, the types of complaints activities. OCRD also reports data to the American public pursuant to No FEAR Act requirements. The No FEAR information is also comprised of numerical data and types of complaints activities.

In addition, OCRD submits administrative case files for cases appealed to the EEOC. These case files contain all PII and sensitive information related to each complaint. These case files are transmitted to the EEOC via secure internet link.

2.3 SYSTEM INFORMATION

2.3.1 Describe the system and its purpose.

iComplaints is currently hosted under a contract with MicroPact, Inc., facilities located at Inc., 12901 Worldgate Drive, Suite 800, Herndon, VA 20170-6014. MicroPact provides a fully managed support infrastructure service including: supporting hardware and software, secure computing facilities, Internet gateway communications security, system administration, and system and application security services.

Users access the iComplaints system via the Internet. All of the logic and processing functionality of iComplaints resides on one or more central servers, with users accessing iComplaints from their PC client Web browsers.

iComplaints is an enterprise level web-based application that provides a broad range of capabilities for inputting, processing, tracking, managing, and reporting on EEO complaint cases. It includes a number of specific features required by USAID for tracking and managing EEO complaint cases. iComplaints also houses supporting documentation relating to single and class complaints of employment discrimination and retaliation complaints authorized by US employment discrimination and whistle blower statutes.

MicroPact developed iComplaints specifically to manage the EEO process in compliance with MD 110 and to generate the Form 462 annual report to the EEOC. iComplaints includes a set of business rules that assists USAID in ensuring compliance with MD 110, EEOC reporting requirements, and 29 CFR 1614. iComplaints is used by

2.3.1 Describe the system and its purpose.

various federal agencies.

OCRD uses iComplaints at USAID headquarters in Washington, DC. The complainants whose information is in the system can be anywhere at USAID offices and missions around the world. The information is collected in paper, emails, and orally during informal and formal complaint processing. The information is inputted into the system by data entry and by loading scanned documents into case records.

EEO Counselors send the data in MS Word and Adobe pdf documents via email to OCRD. EEO Counselors also communicate with the aggrieved and their representatives via email. When OCRD receives the EEO data, OCRD staff copy the documents into the OCRD P: drive, which is accessible by OCRD staff only. OCRD staff then load the documents into iComplaints as MS Word and Adobe pdf documents. OCRD staff members also communicate with complainants and their representatives via email.

Upon request from the EEOC, OCRD provides full administrative files, including all forms and documentation, to the EEOC via secure connection at https://efx.eeoc.gov/usa. The administrative files are downloaded electronically from iComplaints directly into the EEOC File Exchange Server via https://efx.eeoc.gov/usa.

iComplaints is a major application with a moderate NIST security level, because it contains substantial PII including name and date of birth, thus requiring special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

2.3.2 What type of system and/or technology is involved?

(Please check all that apply. If you choose New Technology *or* Other, *please explain.)*

☒ Network
☒ Database
☒ Software
☐ Hardware
☐ Mobile Application or Platform
☐ Mobile Device Hardware (cameras, microphones, etc.)
☐ Quick Response (QR) Code (matrix geometric barcodes scanned by mobile devices)
☐ Wireless Network
☐ Social Media
☐ Advertising Platform
☐ Website or Webserver
☒ Web Application
☐ Third-Party Website or Application
☐ Geotagging (locational data embedded in photos and videos)
☐ Near Field Communications (NFC) (wireless communication where mobile devices connect without contact)

2.3.2 What type of system and/or technology is involved?

(Please check all that apply. If you choose New Technology *or* Other, *please explain.)*

☐ Augmented Reality Devices (wearable computers, such as glasses or mobile devices, that augment perception)

☐ Facial Recognition

☐ Identity Authentication and Management

☐ Smart Grid

☐ Biometric Devices

☐ Bring Your Own Device (BYOD)

☒ Remote, Shared Data Storage and Processing (cloud computing services)

☐ Other:

☐ None

2.3.3 What is the system status?

(If this is an existing Information Collection, please enter the OMB Control Number. If you choose Other, *please explain.)*

☐ New System Development or Procurement

☐ Existing System Being Updated

☐ Existing Information Collection
OMB Control Number:

☐ New Data Collection Form or Survey

☒ Other: Existing system, updating privacy documentation.

2.3.4 Do you use new technology or technology used in ways not previously used by USAID?

(If you choose Yes, *please provide the specifics of any new privacy risks and mitigation strategies.)*

☒ No.

☐ Yes:

2.3.5 Who owns and/or controls the system involved?

(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)

☒ USAID Office: Office of Civil Rights and Diversity

☐ Another Federal Agency:

☒ Contractor: MicroPact, Inc., 12901 Worldgate Drive, Suite 800, Herndon, VA 20170-6014

☒ Cloud Computing Services Provider: MicroPact, Inc., 12901 Worldgate Drive, Suite 800, Herndon, VA 20170-6014

☐ Third-Party Website or Application Services Provider:

☐ Mobile Services Provider:

☐ Digital Collaboration Tools or Services Provider:

☐ Other:

2.3.6 Who is involved in the development and/or continuing operation of the system and/or technology?

(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)

☐ Mobile device manufacturer or other equipment manufacturer:

☒ Application Developer: MicroPact, Inc., 12901 Worldgate Drive, Suite 800, Herndon, VA 20170-6014

☐ Content Developer or Publisher:

☐ Wireless Carrier:

☐ Advertiser:

☐ Equipment or Device Vendor:

☐ Device User:

☐ Internet Service Provider:

☐ Third-Party Data Source (Data Broker):

☐ Other:

3. PRIVACY RISKS AND CONTROLS

3.1 AUTHORITY AND PURPOSE (AP)

3.1.1 Why is the PII collected and how do you use it?

OCRD collects information from direct hires, contractors, applicants, Foreign Service Nationals (FSN)/Locally Employed Staff (LES), and Third Country Nationals (TCN) who believe that they have been subjected to discrimination or harassment/hostile work environment. OCRD uses this information to document individuals who use the EEO complaint process. OCRD collects basic contact information for each complainant and the data necessary to properly process complaints based on race, color, religion, sex, age (40+), national origin, genetic information, or physical or mental disability.

The information collected is used to properly administer and adjudicate EEO complaints, which includes preparing reports. Appropriate action cannot be taken to resolve EEO matters without aggrieved/complainant and/or witness information and factual accounts of alleged incidents.

iComplaints may aggregate data in order to show trends, whether the information is an aggregate of component data, Fiscal Year data, or benchmark data. OCRD uses this information to determine the status of compliance with legal authorities. OCRD also uses the information for internal purposes including complying with statutory, regulatory, or executive reporting requirements relative to departmental attempts to maintain a continuing program to promote equal employment opportunity and eliminate discriminatory practices; extracting relevant testimony and evidence regarding discrimination allegations from testimony of complainants, co-workers, supervisors, potential witnesses and others; providing access to information to legal and lay representatives with defense responsibilities; and providing access to information to supervisor for consideration and/or imposition of personnel or disciplinary action when necessary to comply with remedial order.

3.1.2 What are your processes and procedures for identifying and evaluating any proposed new uses of the PII?

USAID follows all proposed new uses of PII directed by MD 110, 29 CFR 1614, and USAID Automated Directives System (ADS) 110.

3.2 ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (AR)

3.2.1 Do you use any data collection forms or surveys?

(If you choose Yes, *please provide the OMB Control Number and USAID control number.)*

☐ No.

☒ Yes: The following forms are used in the complaint process and with iComplaints. The forms are attached at the end of this PIA.

Notice of Rights and Responsibilities
Notice of Rights and Responsibilities for Non-US Citizen FSN/TCN Staff
Designation of Complainant’s Attorney or Representative AID 110-8
EEO Counseling Contact Form
Agreement to Extend EEO Counseling Time Period AID 110-7
Alternative Dispute Resolution Election Form

3.2.1 Do you use any data collection forms or surveys?

(If you choose Yes, please provide the OMB Control Number and USAID control number.)

USAID EEO Counselor’s Report
Informal or Formal Complaint of Discrimination Withdrawal Form AID 110-5
Notice of Informal EEO Case Closure for Non-U.S. Citizen Foreign Service National (FSN) Employees and Locally Employed Staff (LES)
Notice of Right to File a Formal Complaint AID 110-9
Formal Complaint of Discrimination
Conformation of Request for Reasonable Accommodation
Denial of Reasonable Accommodation Request
Reasonable Accommodation Information Reporting

3.2.2 If the PII is being migrated from a legacy system to a new system, what safeguards are in place to mitigate the privacy risks of transferring the PII from the old to the new system?

Not Applicable.

3.2.3 What privacy requirements have you included in contracts and other acquisition-related documents, pursuant to the Federal Acquisition Regulation (FAR) and compliance with the Privacy Act, FISMA, and other privacy requirements?

The June 12, 2013, USAID contract with MicroPact for services involving iComplaints requires MicroPact to implement the controls contained within the *FedRAMP Cloud Computing Security Requirements Baseline* and *FedRAMP Continuous Monitoring Requirements* for low and moderate impact systems as defined in NIST FIPS PUB 199. The contract also includes by reference the *FedRAMP Standard Contract Language* document.

The *FedRAMP Standard Contract Language* document includes a *FedRAMP Privacy Requirements* section with specific dictates including the use of information that is subject to the Privacy Act that will be utilized in full accordance with all rules of conduct applicable to Privacy Act Information. The *FedRAMP Privacy Requirements* section of the contract also includes sections detailing requirements regarding sensitive information storage, protection of information, confidentiality and nondisclosure, and disclosure of information. The contract and *FedRAMP Standard Contract Language* document is attached at the end of this PIA.

The contract also requires related security maintenance and reporting required to maintain the FISMA certification and accreditation certificate.

3.2.4 What requirements have you included in contracts and other acquisition-related documents to ensure that 1) USAID owns and controls the PII in the system for the length of the contract and beyond, 2) the contractor or service provider has no ownership of the PII, and 3) the contractor or service provider has no access or retention rights to the PII beyond those authorized by the contract during the life of the contract?

The contract includes by reference the *FedRAMP Standard Contract Language* document, and both are attached at the end of this PIA. The *FedRAMP Standard Contract Language* document specifies that disposition of the data will be at the written direction of the Contracting Officer’s Representative: MicroPact shall be responsible for properly protecting all information use, gathered, or developed as a result of work under this contract; USAID will retain unrestricted rights to government data; data must be available to USAID upon request within one business

3.2.4 What requirements have you included in contracts and other acquisition-related documents to ensure that 1) USAID owns and controls the PII in the system for the length of the contract and beyond, 2) the contractor or service provider has no ownership of the PII, and 3) the contractor or service provider has no access or retention rights to the PII beyond those authorized by the contract during the life of the contract?

day; data shall not be used for any other purpose other than that specified in the contract; and no data shall be released by MicroPact without the consent of USAID in writing

3.2.5 How do you audit and/or monitor system and user activity to ensure that the administrative, technical, and physical security safeguards you use actually do guard against privacy risks?

According to the April 20, 2012, Micropact iComplaints System Security Plan, Micropact has categorized iComplaints as a moderate system, pursuant to NIST FIPS PUB 199 and has implemented the appropriate NIST SP 800-53 security controls in the Audit and Accountability family, including AU-1 through AU-8 and AU-12.

In addition, OCRD restricts access to the PII in iComplaints to only those OCRD staff with an official need-to-know. MicroPact has included in iComplaints the ability to monitor user (both MicroPact and OCRD) access and activities through an audit log function. This audit log function tracks users, user's actions with specific description, user's IP address, and the date and time of the actions.

3.2.6 How do you ensure that USAID employees, contractors, and service providers understand their responsibility to protect PII and the procedures for protecting PII?

USAID conducts new employee and new contractor training that includes privacy training.

3.2.7 If you collect PII under a pledge of confidentiality for exclusively statistical purposes, how do you ensure that the PII is not disclosed or used inappropriately?

Not Applicable.

3.2.8 What other risks to privacy exist and how do you manage these risks?

Not Applicable.

3.3 DATA QUALITY AND INTEGRITY (DI)

3.3.1 How do you ensure that you collect information to the greatest extent possible directly from the subject individual?

OCRD collects information directly from the aggrieved or complainants and other individuals involved in the complaint process through forms and interviews

3.3.2 How do you ensure, to the greatest extent possible, that the PII is accurate, relevant, timely, and complete at the time of collection?

OCRD employees or collateral duty EEO counselors assigned to cases verify information with the aggrieved or complainants and other individuals involved in the complaint process through forms and interviews to make sure that it is accurate as they shepherd each case through the complaint process.

3.3.3 How do you check for, and correct as necessary, any inaccurate or outdated PII in the system?

OCRD employees review information to make sure that it is accurate as they shepherd each case through the complaint process.

3.4 DATA MINIMIZATION AND RETENTION (DM)

3.4.1 What are the minimum PII elements that are relevant and necessary to accomplish the legal purpose of the program?

(If you choose Yes*, please explain the business need for the PII elements.)*

OCRD collects and uses only PII that is relevant to the specific complaint presented. For example, race information is not collected for an age discrimination case. OCRD trains OCRD staff and collateral duty EEO counselors to collect only the data that is relevant for each complaint.

If unable to collect, use, maintain, or disseminate the specific PII elements, OCRD would be unable to process the EEO complaints in accordance with Federal regulations.

3.4.2 How do you monitor the PII and the system to ensure that only the PII identified in the privacy notices is collected, used, maintained, and disseminated by the system and that the PII continues to be necessary to accomplish the legally authorized purpose?

OCRD employees or collateral duty EEO counselors only collect PII information pursuant to MD 110 and 29 CFR 1614

3.4.3 Does the system derive new data or create previously unavailable data about an individual through aggregation or derivation of the information collected? Is the PII relevant and necessary to the specified purposes and how is it maintained?

(If you choose Yes*, please explain.)*

☒ No.

☐ Yes:

3.4.4 What types of reports about individuals do you produce from the system?

OCRD tracks and reports to the U.S. Equal Employment Opportunity Commission all USAID EEO activities pursuant to 29 CFR 1614. The reports to the EEOC are comprised of numerical data as well as the types of complaints activities. OCRD also reports data to the American public pursuant to No FEAR Act requirements, comprised of numerical data and types of complaints activities.

In addition, OCRD uses and produces an investigation information document and a decision for each formal complaint; an administrative case file for the EEOC upon request; the documentation in iComplaints to find patterns of discrimination in the agency and its offices and programs; and the information in iComplaints to track case load and case progress within OCRD.

3.4.5 How do you file, maintain, and store the PII? How long do you retain the PII? What methods do you use to archive and/or dispose of the PII? How do you ensure that the records management retention rules specified above are followed?

OCRD uses the National Archives and Records Administration General Records Schedule 1 Civilian Personnel Records (found at http://www.archives.gov/records-mgmt/grs/grs01.html) to determine the filing, maintenance, storage, and retention requirement of the PII collected, used, maintained, and disseminated. Specifically, OCRD follows GRS 1, Item 25 Equal Employment Opportunity (EEO) Records

Generally, OCRD retains EEO complaint records for three years from date of closure and then destroys paper records by shredding and electronic records according to the USAID *ADS 545mas Media Handling Procedures and Guidelines, Mandatory Reference for ADS Chapter 545*, and *ADS 545mak Data Remanence Procedures, A Mandatory Reference for ADS Chapter 545*.

3.4.6 Does the system monitor or track individuals?

(If you choose Yes*, please explain the monitoring capability.)*

☒ No.

☐ Yes:

3.4.7 What policies, procedures, and control methods do you follow to minimize the use of PII for and protect PII during testing, training, and research?

OCRD staff and collateral duty EEO counselors assigned to specific cases are responsible for minimizing the use of PII for those cases. OCRD uses public case law records for all EEO training. OCRD does not use PII during testing or research.

3.5 INDIVIDUAL PARTICIPATION AND REDRESS (IP)

3.5.1 What opportunities for consent do you provide to individuals regarding what PII is collected and how that PII is shared?

There is a mandatory collection of information for any individual who wants to file an EEO complaint. Failure to provide the information may result in the dismissal of a formal complaint; therefore, OCRD must collect this information in order to process complaints. There is also a mandatory collection of information for any federal government official or witness who is involved in providing information regarding the complaints. There is a voluntary collection of information for persons outside the federal government.

3.5.2 What mechanism do you provide for an individual to gain access to and/or to amend the PII pertaining to that individual?

OCRD allows the aggrieved/complainant and other individuals involved in a complaint to file a written request to correct their PII after the informal or formal complaint process.

3.5.3 If your system involves cloud computing services and the PII is located outside of USAID, how do you ensure that the PII will be available to individuals who request access and redress?

The USAID contract with MicroPact for services involving iComplaints includes by reference the *FedRAMP Standard Contract Language* document. The *FedRAMP Standard Contract Language* document includes a *FedRAMP Privacy Requirements* section with specific dictates including that the data must be available to USAID within one business day. The contract and *FedRAMP Standard Contract Language* document is attached at the end of this PIA.

3.6 SECURITY (SE)

3.6.1 How do you secure the PII? What administrative, technical, and physical security safeguards do you use to guard against privacy risks such as 1) data loss or breach; 2) unauthorized access, use, destruction, or modification; 3) unintended or inappropriate disclosure; or 4) receipt by an unauthorized recipient?

OCRD restricts access to the PII in iComplaints to only those OCRD employees with an official need-to-know. Physical access is protected through secure space that uses identification cards, card reader systems, and closed circuit TV. System access requires username and unique password, which can only be authorized by the System Owners.

The contract between USAID and MicroPact for services involving iComplaints requires that PII be disclosed only to authorized personnel on a need-to-know basis. The contract also requires that, when the PII is no longer required, MicroPact return to USAID control, destroy, or hold that PII until otherwise directed, and that the disposition of all data will be at the written direction of the COR. Under the contract, PII must be protected against unauthorized access, disclosure or modification, theft, or destruction and MicroPact must ensure that the facilities that house the network infrastructure are physically secure.

According to the April 2012, MicroPact iComplaints System Security Plan, MicroPact has categorized iComplaints as a moderate system, pursuant to NIST FIPS PUB 199 and has implemented appropriate NIST SP 800-53 security controls in the following control families: AC-Access Control; AT-Awareness and Training; CA-Security Assessment and Authorization Controls; IA-Identification and Authorization; IR-Incident Response; and MP-Media Protection.

The MicroPact IT Administration Team monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. This control is Control Status: Implemented by the routers and firewall systems and coordinated with the Internet Providers. Principal System Components: MicroPact uses Dell PowerEdge servers for the production environment. The Fortigate 620B firewall is used at the boundary as well as to segregate the production environment. The web server is isolated as well through the Fortigate 620B. For Security Software Protection, MicroPact utilizes Trend Micro Enterprise Security Suite to provide protection on the server. The software provides real-time scanning of the system as well as full nightly scans. For Security Protection, access to the system is controlled by Active Directory permissions. External Access to the system is controlled through the Fortigate 620B firewall.

MicroPact has included in iComplaints the ability to monitor user (both MicroPact and OCRD) access and activities through an audit log function. This audit log function tracks users, user’s actions with specific description, user’s IP address, and the date and time of the actions.

iComplaints is a role-based system. In this type of system, a user's access and available functions are determined by the role assigned to the user. Roles are created by the master administrator and have specific rights and privileges assigned to them when created. By default, the system has an Administrator and a Super Processor. Only the Master Administrator can assign a user the Administrator and Super Processor roles. Because privileges assigned to a role determine system capabilities available to a user, they also determine the screens, navigation buttons, and links displayed to the user. The role assigned to a user is "checked" by the system when the user logs in, and the corresponding screens, buttons, etc. are displayed.

3.6.2 If your system is controlled by a contractor or service provider, what requirements have you included in contracts and other acquisition-related documents to detail the procedures for privacy breach liability and response?

The contract between USAID and MicroPact for services involving iComplaints includes a section on security incidents, which requires both parties to notify the other party immediately by telephone or email when a security incident is detected. The contract also requires MicroPact to provide a copy of the System Security Plan for iComplaints. MicroPact has developed an Incident Response Plan, dated July 19, 2012, which provides the elements of the MicroPact security incident response procedures.

3.7 TRANSPARENCY (TR)

3.7.1 How do you provide notice to individuals regarding 1) the authority to collect PII; 2) the principal purposes for which the PII will be used; 3) the routine uses of the PII; and 4) the effects on the individual, if any, of not providing all or any part of the PII?

One government-wide SORN provides public notice for the OCRD collection, use, maintenance, and dissemination of PII related to EEO complaints:

EEOC/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeals Records, 67 FR 49338 (July 30, 2002)

Also, OCRD has a Privacy Act statement on the following forms:

USAID EEO Counselor’s Report
Formal Complaint of Discrimination

3.7.2 Have you or will you publish a Privacy Act System of Records Notice (SORN) for this system?

(If you choose Yes*, please provide information about the SORN, including the name, date, and Federal Register citation.)*

☐ No

☒ Yes:

EEOC/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeals Records, 67 FR 49338 (July 30, 2002), (available at http://www.gpo.gov/fdsys/pkg/FR-2002-07-30/pdf/02-18895.pdf)

3.7.3 If your system involves cloud computing services and the PII is located outside of USAID, how do you ensure that you know the location of the PII and that the SORN System Location(s) section provides appropriate notice of the PII location?

The primary iComplaints work location is at MicroPact, Inc., 12901 Worldgate Drive, Suite 800, Herndon, VA 20170-6014. The contract between USAID and MicroPact for services involving iComplaints states that it is anticipated the iComplaints information will be gathered, created, and stored within the primary work location. The contract also states that, if MicroPact personnel must remove any information from the primary work area, they should protect it to the same extent they would their proprietary data and/or company trade secrets.

3.8 USE LIMITATION (UL)

3.8.1 How do you monitor access to and use of the system to ensure that the PII is collected, accessed, and used only 1) for the authorized purposes and 2) by authorized USAID employees, contractors, and service providers?

The iComplaints System Owner restricts access to only those with a business need-to-know. Each iComplaints user has a unique password that is different than their AIDNet password. The System Owner also assigns specific levels of access to users.

According to the April 2012 MicroPact iComplaints System Security Plan, Micropact has categorized iComplaints as a moderate system, pursuant to NIST FIPS PUB 199 and has implemented appropriate NIST SP 800-53 security controls in the following control families: AC-Access Control; and IA-Identification and Authorization.

3.8.2 If you share PII outside of USAID, how do you ensure the protection of the PII 1) as it moves from USAID to the outside entity and 2) when it is used, maintained, or disseminated by the outside entity?

(If you choose Yes, please provide the specifics of the agreement or a copy of the agreement.)

Upon request from the EEOC, OCRD provides full administrative files, including all forms and documentation, to the EEOC via secure connection at https://efx.eeoc.gov/usa. OCRD sends paper copies of documents to complainants and their attorneys or representatives via certified mail. OCRD uses email transactions to send information to the aggrieved/complainant and their attorneys or representatives. OCRD will follow the USAID policy that all PII must be put in an encrypted attachment when sending PII in an email message outside USAID.

3.9 THIRD-PARTY WEBSITES AND APPLICATIONS

3.9.1 What PII might become available to you when the third-party website or application makes information available to you through public use?

Not Applicable

3.9.2 How do you ensure that the privacy policy of the third-party website and/or application is reviewed to ensure that it appropriately supports the USAID privacy protection position?

Not Applicable.

3.9.3 If you have a link from USAID.gov to this third-party website or other location that is not a part of an official government domain, do you provide an alert (such as a statement or “pop-up”) to visitors explaining that they are being directed to a non-governmental website that may not afford the same privacy protections as USAID?

Not Applicable.

3.9.4 If you incorporate or embed the third-party application on the USAID website, how do you disclose to the public the third-party application?

(If you choose Yes*, please describe the disclosure.)*

Not Applicable

3.9.5 How do you create the appropriate USAID brand to indicate an official USAID presence on the third-party website, and how you distinguish USAID activities from those of non-governmental actors?

Not Applicable